COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, June/juin 2011 T-PD-BUR(2011) 01 MOS rev 6

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL [STE n°108]

(T-PD-BUR)

"Consultation concerning the modernisation of Convention 108: results"

"Consultation relative à la modernisation de la Convention 108 : résultats"

Secretariat document prepared by
the Directorate General of Human Rights and Legal Affairs

Document préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

INDEX

INTRODUCTION

On the occasion of the 5th data protection day (28 January 2011), the Council of Europe launched a public consultation aimed at allowing interested persons and institutions to send to the Secretariat their comments, thoughts, ideas on the modernisation of Convention 108.

A consultation paper[1] was published on the Council of Europe website and advertised in press releases.

A total of 50[2] replies has been received. A compilation has been prepared which will be examined by the Bureau of the Consultative Committee of Convention 108 in the framework of its modernisation work of Convention 108.

A l'occasion de la 5ème journée de la protection des données (le 28 janvier 2011), le Conseil de l'Europe a lancé une consultation publique sollicitant les personnes et organisations intéressées à envoyer au Secrétariat leurs commentaires, réflexions et idées au sujet de la modernisation de la Convention 108.

Une note de consultation[3] a été publiée sur le site du Conseil de l'Europe et relayée dans des communiqués de presse.

Un total de 50[4] réponses a été reçu. Une compilation a été préparée et sera examinée par le Bureau du Comité Consultatif de la Convention 108 dans le contexte de son travail sur la modernisation de la Convention 108.

[1] http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf

[2] In the date of 12 May 2011

[3] http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_FR.pdf

[4] A la date du 12 mai 2011

SYNTHESE DES COMMENTAIRES RECUS

(ENGLISH VERSION FOLLOWING)

Introduction

1. La consultation publique lancée par le Conseil de l'Europe pour recueillir les réactions de toutes les parties concernées sur la perspective de modernisation de la Convention 108 a remporté un franc succès. De nombreuses contributions sont parvenues au Secrétariat du Conseil de l'Europe. Ces contributions sont le plus souvent approfondies et étayées par des arguments ou analyses bénéficiant de l'expertise ou de l'expérience de terrain des contributeurs. Par ailleurs, certains intervenants se sont groupés pour présenter une réaction commune au questionnaire et d'autres, en tant que fédérations ou groupements, se sont exprimés au nom de tous leurs membres.
2. Tous les horizons sectoriels sont représentés parmi les répondants : des acteurs issus tant du secteur public (autorités gouvernementales, autorités de protection des données,…) que du secteur privé (monde bancaire, des assurances, du commerce électronique, du marketing, de la diffusion audio-visuelle, de la recherche socio-économique,…), ainsi que du monde universitaire et des associations intéressées.
3. Une représentation géographique variée s'observe aussi. Ainsi, les réponses proviennent des différentes zones de l'Europe. Les pays de l'Union européenne sont concernés mais également des pays hors de l'UE, comme l'Albanie ou l'Ukraine. Il est intéressant de pouvoir comparer les réponses issues de pays couverts par la directive européenne relative à la protection des données (zone UE) avec celles venant d'autres pays qui ne le sont pas. Par ailleurs, des contributions sont parvenues d'Amérique du Nord (Etats-Unis et Canada), de l'Afrique (Sénégal, Ile Maurice), de l'Australie. L'organisation internationale de la Francophonie a également émis un commentaire.

Considérations générales

4. Parfois les réponses obtenues signalent une orientation à suivre mais n'apportent pas d'indication sur le moyen de concrétiser cette orientation. Parfois, au contraire, les commentateurs présentent des arguments et des pistes pour aller dans telle ou telle direction.
5. Dans une série de cas, les contributeurs annoncent qu'au vu de la difficulté de la question, il conviendrait de réaliser une étude approfondie. C'est le cas par exemple pour l'exclusion du champ d'application des traitements de données à des fins personnelles et domestiques ou pour la question du droit applicable. Dans d'autres cas, c'est à une analyse d'impact ou à une étude d'efficacité des mesures législatives envisagées qu'invitent les contributeurs (notamment concernant l'introduction de la possibilité des recours collectifs et de systèmes d'*alternative dispute resolution*, ou concernant l'instauration d'un devoir de signaler les violations de données – *data breaches*).
6. De très nombreux contributeurs ont plaidé pour que le travail de modernisation de la Convention soit effectué en ayant le souci d'établir la plus grande cohérence avec les règles de protection édictées par l'Union européenne (principalement la directive 95/46). Dans bien des cas les réponses sont donc orientées par cette préoccupation d'aligner le texte de la Convention sur celui de la directive européenne. Il est demandé de suivre les travaux de

modernisation de cette directive actuellement en cours pour veiller à ne pas faire naître des divergences entre les textes. Il est intéressant de souligner que cette préoccupation n'est pas formulée par les seuls acteurs issus de pays de l'Union européenne. Elle est partagée par des acteurs situés hors de l'UE.

Objet et champ d'application de la Convention, Définitions

1. Rédigée selon une approche « technologiquement neutre », la Convention 108 est un instrument général et simple : peut-on conserver cette approche ou doit-on au contraire élaborer un texte plus détaillé ?

7. L'ensemble des répondants s'est prononcé en faveur du maintien d'un texte simple, énonçant des principes généraux.
8. Cette approche est à leurs yeux la seule qui puisse garantir la viabilité à long terme de la Convention. Les trente années écoulées avec une Convention consacrant des principes généraux ont démontré que ce modèle passait positivement l'épreuve du temps.
9. Dans la même perspective de durée, tous soulignent également la nécessité de veiller au caractère technologiquement neutre de la Convention. La formulation des principes ne doit pas être focalisée sur l'existence d'une technologie. Cela présenterait le double risque de désuétude des principes dès que la technologie sera dépassée ou abandonnée et d'inadaptabilité de ces principes aux nouvelles technologies qui ne manqueront pas d'émerger.
10. Cela étant dit, les répondants indiquent que, tout en ne transformant pas le texte de la Convention en un texte trop détaillé, il s'impose tout de même d'apporter certains compléments au texte existant.
11. Plusieurs contributeurs attirent l'attention sur le fait que si la Convention doit désormais avoir une vocation universelle, il faut être conscient qu'un texte trop détaillé fera assurément peur aux Etats qui envisageraient leur éventuelle adhésion à la Convention.
12. Le modèle existant devrait donc être poursuivi, selon certains : conserver un caractère général et simple au texte de la Convention et détailler les principes généraux dans des textes spécifiques (recommandations du Comité des ministres).

2. La Convention 108 devrait-elle définir le droit à la protection des données et le droit au respect de la vie privée ?

13. Certaines des personnes ayant répondu à cette question estiment qu'intégrer des définitions du droit à la protection des données et du droit au respect de la vie privée aiderait à clarifier la portée du texte et aiderait le public à percevoir le champ de la matière. Cela mettrait notamment en lumière, aux yeux de l'APEP – Association Professionnelle Espagnole de la Vie privée, que la vie privée et la protection des données sont deux droits différents, les données à caractère personnel pouvant d'ailleurs être privées ou non.
14. D'autres estiment que la notion de vie privée apparaissant dans plusieurs instruments juridiques internationaux, il ne serait pas opportun de la définir dans la Convention 108. Il appartient à la Cour européenne des droits de l'homme, notamment, de définir la portée de cette notion reprise à l'article 8 CEDH. Pour la CNIL, par exemple, il ne faut pas définir ces notions pour leur permettre d'être interprétées de façon évolutive. Le State Data Protection

Inspectorate de Lituanie relève que les instruments juridiques internationaux qui protègent la vie privée ne contiennent aucune définition de celle-ci. La même approche pourrait être suivie en ce qui concerne le droit à la protection des données.

15. Signalons au passage que les contributions laissent entrevoir une perception non homogène de ce qu'est la vie privée/privacy. Dans plusieurs contributions, c'est l'évocation du sens classique (intimité, confidentialité) qui est mentionnée et non le sens plus évolué d'autonomie et de maîtrise informationnelle qui a été mis au jour par la Cour européenne des droits de l'homme. La European Banking Association qui estime que la Convention 108 devrait contenir les définitions en question précise d'ailleurs que cela doit être particulièrement fait dans la mesure où la Convention doit servir de base à des pays situés hors de la zone de l'Espace Economique Européen et qui ne disposent pas de définitions spécifiques dans leur propre législation et n'ont aucune connaissance de l'évolution des notions de « vie privée/privacy » et de « protection des données » dans la jurisprudence et la doctrine en lien avec les définitions européennes existantes.
16. Par contre, pour ce qui est de la notion de droit à la protection des données, ces contributeurs et d'autres perçoivent l'intérêt d'une définition tout en incitant à l'harmoniser avec celle se trouvant dans la Charte des droits fondamentaux de l'Union européenne. Privacy International souligne en ce sens qu'il vaudrait la peine de songer à définir le droit à la protection des données étant donné que de nombreuses constitutions dans le monde ont commencé à reconnaître que la protection des données est effectivement un droit.
17. Certains répondants trouvent qu'il ne se justifie pas de définir les notions après 30 ans d'application du texte. L'ancienneté du texte fait réagir dans un sens opposé la Direcçao Geral da Politica de Justiça du Portugal qui estime qu'en tant que le plus ancien instrument juridique de droit international public en la matière, la Convention 108 qui prétend régler le droit à la protection des données ne peut se montrer incapable de définir elle-même ce droit.
18. Ne se prononçant pas sur l'opportunité d'introduire de telles définitions, l'European Newspaper Publishers Association demande que si l'on opte pour une définition, on veille à ne pas induire que ces droits prévaudraient sur ceux de la liberté d'expression et d'information. Il faut également veiller à ne pas introduire d'insécurité juridique.

3. La Convention 108 protège les individus contre toute atteinte portée à leur vie privée par des autorités privées et publiques, y compris la police et la justice. Cette approche globale doit-elle être conservée ?

19. Il y a unanimité pour considérer qu'il faut conserver une approche couvrant tant le secteur privé que l'ensemble du secteur public, incluant donc la police et la justice. Etant donné les facilités pratiques et le potentiel des outils techniques existants (sans compter ceux qui apparaîtront à l'avenir), il est considéré comme « absolument vital », pour reprendre les termes de nombre de contributeurs, d'imposer aux acteurs de la police et de la justice le respect de principes de protection des données.
20. Bien sûr tout le monde s'accorde sur la nécessité d'aménagement de ces principes pour prendre en compte les nécessités liées au travail de ces acteurs. L'important est de ne pas faire sortir purement et simplement la justice et la police du champ de la protection. Ce qui est envisagé c'est généralement un régime d'exceptions partielles au bénéfice de ces acteurs.

21. TechAmerica Europe propose que l'on réfléchisse à des situations dans lesquelles des règles différentes partielles existeraient pour les autorités publiques et pour les entités privées, tout en gardant les mêmes principes de base et exigences de transparence. Ils invitent à prendre en considération l'impact que les modifications de la Convention pourront avoir sur le travail de la police et de la justice pour vérifier que ces nouvelles mesures ou nouveaux concepts ne suscitent pas des difficultés particulières pour ce secteur.
22. Un autre contributeur américain demande que l'on soit attentif à ce que tout changement que l'on apporterait à la Convention continue de permettre un degré de flexibilité des échanges de données « policières » entre Etats-Unis et Europe et autorise le partage de données à des fins de sécurité publique et de poursuite des infractions.
23. Les contributeurs canadiens ont souligné que l'expérience de deux régimes séparés pour les secteurs public et privé qu'ils connaissent au niveau fédéral chez eux a fait l'objet de critiques émanant de la société civile et du *Federal Privacy Commissioner*.

4. La Convention 108 n'exclut pas de son champ d'application les données traitées par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. Doit-on maintenir cette approche, ou au contraire introduire une exception dans ce cas précis (dans le contexte spécifique du Web 2.0.) ?

24. De façon générale les répondants sont favorables à l'introduction d'une exclusion du champ d'application de la Convention des traitements de données effectuées à des fins personnelles ou domestiques.
25. De nombreux répondants soulignent que cela doit se faire dans le souci d'aligner le modèle de protection de la Convention sur celui de la directive 95/46.
26. Toutefois plusieurs contributeurs sont d'avis qu'il sera particulièrement difficile de définir ce qui serait précisément visé par une telle exclusion.
27. L'AEDH, favorable à cette exclusion, propose de la soumettre à la condition qu'il n'y ait pas transmission de données à des tiers et d'accompagner cette exclusion d'une obligation pour les services qui serviraient de support à de telles activités personnelles (messagerie électronique, carnet d'adresses, agenda, service d'archivage,…) d'informer leurs clients sur leurs obligations et de leur offrir des fonctions de confidentialité.
28. La CNIL invite à reprendre le modèle de l'Union européenne et dire qu'il relève du pouvoir d'interprétation des autorités de contrôle nationales de préciser ce qui relève ou non de l'exception.
29. Le CIPPIC (Canada) relève que cette question a été mentionnée comme un des défis à venir en matière de protection des données. Il convient en tout cas d'effectuer une prudente mise en balance avec le droit à la liberté d'expression lorsque l'on veut régler cette question du sort des activités privées des individus. C'est précisément à l'occasion de leur réflexion sur la liberté d'expression confrontée à la protection des données que le Centre for Socio-Legal Studies a développé son point de vue sur cette hypothèse d'exclusion. Réalisant que beaucoup de situations dans lesquelles des données personnelles sont traitées de la façon la plus intrusive et la plus injustifiable sont de plus en plus souvent le fait de personnes privées mues par des raisons non commerciales, ce Centre ne souhaite pas voir ces activités exclues de toute règle de protection. A ses yeux une meilleure solution consisterait d'abord à s'assurer que de telles activités individuelles puissent bénéficier pleinement d'une disposition nouvelle plus large sur la liberté

d'expression et ensuite à imposer aux individus seulement certaines des obligations des responsables de traitement, déterminées de manière claire et proportionnée.

30. La European Privacy Association, rejointe sur ce point par l'APEP (Association Professionnelle Espagnole de la Vie privée) et par le State Data Protection Inspectorate de Lituanie, soulève que les activités des individus peuvent aujourd'hui porter facilement atteinte à d'autres et qu'on ne peut donc exclure totalement leurs activités des règles de protection des données. Mais par contre, on ne peut soumettre des activités purement personnelles à des obligations et charges disproportionnées, notamment en matière de sécurité (article 7) et concernant les flux transfrontières (article 12). L'APEP insiste sur le fait que la régulation doit pouvoir sanctionner les usages abusifs de données à caractère personnel commis par des particuliers. Cette association estimerait pour sa part disproportionné que l'on impose aux utilisateurs particuliers des obligations telles que celle de déclarer le traitement de données, de fournir des informations dans la ligne des articles 10 et 11 de la directive 95/46, d'adopter des mesures de sécurité ou de veiller à ce que de telles mesures soient implémentées par la plateforme qu'ils utilisent.

31. La Commission à la protection des données du Sénégal suggère qu'au-delà de l'exclusion proposée qu'elle soutient, on élargisse cette exclusion en y ajoutant « les traitements dont les données ne sont pas destinées à une communication systématique à des tiers ou à la diffusion ».

5. La définition du traitement automatisé n'inclut pas la collecte des données : le fait que la collecte fasse l'objet d'une disposition spéciale est-il problématique ? Est-ce suffisant ? Doit-on ajouter d'autres opérations à la liste existante ?

32. Tous ceux qui se sont exprimés sont favorables à l'inclusion de la notion de collecte dans celle de traitement automatisé. C'est tout d'abord la volonté de garantir une cohérence avec les normes européennes, nationales et internationales qui motive cette position. Ensuite, c'est la conviction qu'il est utile que la collecte soit soumise à l'ensemble des principes régissant les traitements de données et non à une seule disposition particulière.

33. Le souci de cohérence entre les ordres juridiques explique aussi que de nombreux contributeurs comme le CEA Insurers of Europe ou l'AFME BBA (banking & financial services) réclament l'adoption de la notion de « traitement » (« *processing* ») telle que présentée dans la directive européenne. Pour le CEA, il serait utile que l'opération de « communication par transmission » (« *disclosure by transmission* »), opération fondamentale dans le traitement des données, soit expressément reprise dans la liste des opérations couvertes. Pour la CNIL, la notion de traitement devrait être la plus large possible, tant les opérations réalisées sur les données ont tendance à se multiplier et se diversifier.

34. L'AFME BBA de même que l'European Banking Federation relève qu'il faut s'assurer que la terminologie ne soit pas confinée à des concepts comme celui de « fichier » qui ont une connotation technologique datée qui pourrait compromettre à la fois la neutralité du texte et une large application de la Convention, étant donné que cette notion n'a plus de pertinence dans la réalité d'Internet et du *cloud computing*.

35. Enfin, la Direcçao Geral da Politica de Justiça du Portugal invite à réfléchir à l'élargissement du champ d'application de la Convention afin d'y inclure les traitements non automatisés. Conscient que ces traitements sont minoritaires aujourd'hui, cet organe estime toutefois

qu'ils n'ont pas entièrement disparu et que la prudence indique de les intégrer dans le champ de la protection.

La définition du maître de fichier devrait être revue : plusieurs critères doivent-ils être répertoriés, ces critères doivent-ils se cumuler, peut-il y avoir plusieurs maîtres de fichier pour un seul fichier?

36. Pour certains répondants, la Convention dans sa version actuelle ne doit pas être amendée sur ce point. Les définitions actuelles suffisent à rendre responsables les personnes impliquées dans le traitement des données.
37. Pour d'autres, la définition du « responsable du traitement/data controller » issue de la directive 95/46 devrait se substituer à celle de maître de fichier.
38. Le Commissaire à la protection des données de l'Ile Maurice propose de renouveler la définition par la définition suivante : « le maître du fichier est toute personne physique ou morale, publique ou privée, qui décide de toute activité, automatisée ou non, entreprise sur des données personnelles. ». L'APEP - Association Professionnelle Espagnole de la Vie privée propose pour sa part de revoir la définition de manière à inclure « celui/ceux qui de facto a/ont le droit de décider du but et des moyens du traitement de données à caractère personnel, soit par effet de la loi, soit en vertu d'accord contractuel avec la personne concernée ou avec un tiers. ». Par souci de sécurité juridique, cet organisme trouve important que l'on limite les responsables de traitement aux personnes ayant la personnalité juridique.
39. Plusieurs signalent qu'il serait opportun de prévoir l'hypothèse où il y a plusieurs responsables pour un même traitement de données. L'AEDH donne l'exemple de la décision de mise en œuvre d'un fichier prise par un ensemble de responsables à des fins collectives, comme l'élaboration d'un fichier commun à une profession relatif à des clients défaillants. L'APEP fait la distinction entre les contrôleurs joints (en cas de traitement des mêmes données dans le même but) et plusieurs contrôleurs (en cas de traitement des mêmes données mais dans des buts différents).
40. La European Privacy Association attire l'attention sur le fait que de plus en plus les technologies développées (comme celle du *cloud*) conduisent à ce que des données soient traitées de manière automatisée par de multiples intervenants. Pour cette association, il est important non de définir le nom et le rôle de ces intervenants mais plutôt leurs activités de traitement, les charges et obligations en lien avec ces activités et les responsabilités liées. Le Information Commissioner for the United Kingdom's (ICUK) abonde dans le même sens lorsqu'il dit que, plutôt que lister des critères concernant ce qui constitue un « *controller* », il préfèrerait que l'on fournisse une meilleure description des activités qu'un maître de fichier peut entreprendre.
41. Pour EFAMRO ESOMAR (secteur de la recherche), il faudrait introduire une définition clarifiée du "responsable du traitement" qui placerait les responsabilités sur ceux qui décident comment les données vont être traitées par opposition à ceux qui contrôlent un système informatique ou un fichier particuliers. Cela ferait reposer sur un seul responsable du traitement la responsabilité d'évaluer la nécessité de traiter des données et la sécurité des systèmes disponibles avant d'opter pour le traitement de données avec de tels systèmes. Cela assurerait en outre un point unique de responsabilité et d' « accountability » pour les citoyens.

42. La German Insurance Association accueillerait favorablement une révision de la notion de maître du fichier car cela donnerait l'opportunité d'introduire des changements dans le traitement des données dans le monde des affaires. C'est principalement la centralisation des tâches de service au sein des groupes et le recours à l'outsourcing de tâches à des services compétents qui sont concernés. Pouvoir présenter l'entité qui transfère les données et celle qui les reçoit de manière jointe comme un responsable unique du traitement faciliterait les transferts de données et simplifierait la vie des groupes.

43. Cette position va dans le même sens qu'une remarque du consortium Computer Law and Security Review, International Association of IT Lawyers and the Institute for Law and the Web (University of Southampton) : ils relèvent que dans un environnement en réseau, la notion de responsable du traitement n'a plus la pertinence d'antan, étant donné l'usage croissant de systèmes de partage et de mise en relation de données. Dans de tels environnements, il serait préférable de nommer une seule entité comme assumant la responsabilité générale (comme dans les systèmes de *binding corporate rules* de l'UE). Il conviendrait d'imposer l'obligation aux responsables de traitement individuels d'informer les personnes concernées des partages et mises en relation de données auxquels ils participent ainsi que des coordonnées de l'entité de coordination.

44. Enfin, Mydex Community Interest Company signale – et dit que sa vision est partagée par de nombreux autres, incluant le World Economic Forum – qu'à l'avenir les architectures techniques des prochaines générations placeront les individus au centre de leur propre éco-système de données à caractère personnel, assumant donc eux-mêmes le rôle de responsable de traitement. La législation devra refléter ce nouveau modus operandi et permettre ce « data empowerment by design ».

6. De nouvelles définitions sont peut-être nécessaires, comme celle du sous-traitement ou celle du fabricant des équipements techniques.

45. Les contributeurs saluent l'intention d'introduire de nouvelles définitions si cela se fait dans un souci de cohérence avec celles développées au sein de l'UE. Cela permettrait d'augmenter la sécurité juridique, d'améliorer la protection des personnes concernées et d'éviter de créer la confusion pour les responsables de traitement.

46. Plusieurs signalent avec bon sens qu'il est clair qu'il n'y a de sens à insérer la définition d'acteurs supplémentaires que si un régime juridique particulier fixant des obligations est attaché à ces nouveaux acteurs.

47. Plusieurs estiment indispensable l'ajout de la définition du sous-traitant. Le Garante per la protezione dei dati personali italien relève en outre que le besoin d'introduire une telle définition s'est déjà fait sentir dans plusieurs résolutions du Conseil de l'Europe (la Recommandation 2002(9) sur la protection des données dans le secteur des assurances et la Recommandation 2010(13) sur le profilage).

48. Pour Privacy International, par contre, le concept de « sous-traitant » n'est plus utile étant donné que des sous-traitants, dans la réalité, doivent assumer de si nombreux devoirs de sécurité et de respect de la vie privée que leur rôle devient très difficile à distinguer. Il est problématique de demander à des responsables de traitement d'être responsables des mesures de vie privée et de sécurité alors que dans les faits ils sont entièrement dépendants des conditions contractuelles établies par des fournisseurs de service (du *cloud* notamment) non soumis à la régulation.

49. La German Insurance Association demande que cette définition soit flexible et autorise, selon les circonstances, que la maison mère puisse aussi être mandatée par une société du groupe comme sous-traitant, mais que, dans ce cas, il y ait des limites pour reconnaître le droit d'émettre des instructions selon le droit existant.

50. L'AEDH propose qu'une nuance soit introduite pour les fournisseurs de service traitant des données pour le compte du responsable du traitement mais jouissant d'une claire autonomie pour réaliser le service, de sorte qu'ils portent une double casquette de responsable du traitement et de sous-traitant. Dans cette hypothèse, on pourrait introduire la notion de "person entrusted" "personne chargée" du traitement, à qui le traitement est confié: lorsque le sous-contractant agit strictement au nom et sur les instructions du responsable du traitement et n'est pas responsable comme un responsable de traitement, la personne chargée du traitement pourrait être considérée comme supportant une part de la responsabilité, conjointement ou totalement.

51. Pour le ICUK, la simple distinction entre un responsable et un sous-traitant ne reflète plus les relations compliquées qui existent entre les organisations qui traitent des données personnelles. Le modèle des définitions de la directive 95/46 correspond à un sous-traitant passif n'agissant que sur instructions du responsable, alors que dans la réalité celui qui apparaît comme un sous-traitant peut exercer une influence considérable sur la manière dont le traitement prend place et peut, sur bien des aspects, agir comme un responsable de traitement. Pour la CNIL, cette situation où effectivement, de façon croissante, le traitement effectif et quotidien des données se situe dans les mains du sous-traitant et non dans celles du responsable de traitement, conduit à imposer de définir cette catégorie d'acteur. Pour cette autorité, une cohérence avec la définition de la directive précisant qu'il s'agit de l'organisme « agissant pour le compte » du responsable de traitement est nécessaire. Cet organisme plaide encore pour que le régime de responsabilité du sous-traitant soit davantage harmonisé et encadré au niveau européen.

52. Quant à l'ajout d'une définition du "fabricant d'équipements techniques", certains comme l'European Banking Association estiment que c'est une bonne approche de l'envisager, alors que pour l'AEDH, c'est carrément indispensable, que les équipements en question soient matériels ou logiciels. Le Cyberspace Law and Policy Centre (Australie) de même que le Commissioner for Personal Data Protection de Chypre et le consortium CLSR-IAITL-ILAWS notent que cela s'avérera nécessaire si l'on introduit des dispositions concernant le *Privacy by Design* – ce que l'autorité chypriote ne souhaite pas à l'inverse des autres.

53. Le Garante italien a une approche plus nuancée : il estime qu'il serait indubitablement utile d'édicter les garanties qui devraient être offertes par toute entité additionnelle qui prendrait part au traitement d'une façon ou d'une autre (tel que le fabricant d'équipement technique), tout en faisant peser sur le responsable du traitement l'obligation juridique de vérifier le respect de ces garanties.

54. Pour Privacy International, par contre, il ne serait pas sage de définir les fabricants d'équipement hors d'un risque spécifique pour la vie privée et d'un contexte de sécurité. La Direcçao Geral da Politica de Justiça du Portugal est elle aussi opposée à l'inclusion de cette notion, n'en voyant pas l'utilité.

Principes de protection

7. De nouveaux principes pourraient être ajoutés à la Convention, comme le principe de proportionnalité qui devrait s'appliquer à l'ensemble des opérations réalisées sur les données. Ce principe est également lié au principe de minimalisation des données qui vise à limiter la collecte des données à caractère personnel au strict minimum, voire à y mettre un terme quand cela est possible.

55. Pour beaucoup, le principe de proportionnalité est déjà compris dans l'article 5 de la Convention. Ils réduisent donc ce principe à son application quant aux données qui doivent être pertinentes et non excessives.

56. D'autres répondants trouvent qu'il serait recommandable d'inclure les principes de proportionnalité et de minimisation ou limitation de la collecte des données dans les principes de protection, certains disant que ces principes doivent passer de la forme implicite à une formulation explicite. La formulation expresse de ces principes permettrait d'en définir précisément et mieux l'étendue. Notamment cela permettrait de stipuler que le principe de proportionnalité s'applique à toutes les opérations et pas seulement à la collecte (Cyprus Commissioner). Autrement dit, le principe de proportionnalité lié à la finalité de chaque opération du traitement (Garante) ou le critère du caractère non excessif de l'ensemble d'un projet de traitement de données particulier au regard des libertés et droits fondamentaux en cause doit être posé, cumulativement à la nécessité de minimiser les données traitées (AEDH). Dans le même sens l'AEDH dit que le principe de minimisation des données ne doit pas remplacer celui de proportionnalité car celle-ci doit dépasser les seules données.

57. Certains contributeurs appuient fortement l'insertion de ces principes qu'ils estiment très importants (CLPC, Australie ; APEP-Association Professionnelle Espagnole de la Vie privée ; Czech Office for personal data protection ; CLSR-IAITL-ILAWS ; Garante italien).

58. Morpho-Groupe Safran (technologies d'identification) qui voit dans le principe de proportionnalité un principe « qui vise à assurer un équilibre entre le traitement des données et la finalité poursuivie » se méfie de la démarche subjective qu'implique l'application de ce principe. Cette subjectivité débouche sur des divergences entre autorités de protection des données nationales dans l'acceptation ou non d'un produit ou dispositif industriel. Ils souhaitent en conséquence que si ce principe était consacré dans la Convention, il s'accompagne de dispositions de nature objective, telles qu'encourager le recours à des procédures de labellisation/certification reposant sur des critères précis que l'industriel devrait respecter pour développer ses produits.

59. Pour la GDD (association allemande pour la protection des données et la sécurité des données), il faudrait accorder certains avantages aux organisations qui recourent à des pseudonymes plutôt qu'à des données directement reliées à des personnes.

60. ARD et ZDF (radio et télévision) estiment qu'alors que l'utilisateur de médias traditionnels a toujours bénéficié d'un complet anonymat, cela n'est plus vrai pour les services proposés via Internet. En conséquence, ils soutiennent fermement le principe de limiter strictement la collecte de données au but poursuivi.

61. CEA Insurers of Europe demande que la minimisation des données soit présentée comme un objectif et non comme une obligation.

8. La question du consentement devrait-elle être envisagée en étroite liaison avec le principe de transparence et l'obligation d'informer, ou en tant que condition nécessaire à satisfaire un traitement loyal et licite avant toute autre action ?

62. Pour plusieurs contributeurs, il faut relativiser le rôle du consentement comme base légale pour le traitement de données. En tout cas il ne devrait pas servir comme seule base. Pour certains il ne devrait pas être présenté du tout comme condition pour satisfaire un traitement loyal et licite. Dans bien des cas les personnes qui consentent ne se rendent pas compte de ce à quoi elles ont consenti. Le consentement n'est ni une garantie de protection pour les personnes concernées, ni une solution praticable pour les responsables de traitement pour qui il peut représenter un fardeau disproportionné (dans le monde du marketing ou celui des assurances, par exemple).
63. Une grande peur règne quant à la qualité du consentement. Des problèmes de vraie liberté du consentement sont pointés, de même que par rapport à la forme que l'on donne de plus en plus au consentement.
64. Sur ce point, la GDD (association allemande pour la protection des données et la sécurité des données) estime que le modèle de la loi allemande en la matière offre une bonne protection aux consommateurs. Cette loi stipule que si le consentement est donné dans une forme différente que par écrit, le responsable du traitement doit donner une confirmation écrite de la substance du consentement à la personne concernée, à moins que le consentement ait été donné sous forme électronique, auquel cas le responsable doit conserver un enregistrement du consentement auquel la personne concernée doit pouvoir accéder et qu'elle peut révoquer à tout moment avec effet pour le futur.
65. Le CLPC (Australie) propose, quant à lui, le modèle de la loi canadienne régulant la protection de la vie privée dans le secteur privé (PPIPEDA). Une proposition d'amendement de cette législation est particulièrement intéressante : « le consentement d'un individu est seulement valide s'il est raisonnable de s'attendre à ce que l'individu comprenne la nature, le but et les conséquences de la collecte, de l'utilisation ou de la divulgation de l'information personnelle auxquelles il consent ». Pour le CLPC, si on introduit la notion de consentement, il faut que celui-ci soit expressément défini comme libre, informé et révocable, et non lié à d'autres consentements. Il faudrait également un principe général disant que lorsqu'un consentement véritable est une option réaliste, il devrait être le fondement privilégié d'un traitement légitime, ce qui serait cohérent avec le but global de transparence des traitements de données à caractère personnel.
66. La US Federal Trade Commission relève qu'éliminer le choix des personnes concernées pour les pratiques évidentes pour les consommateurs, permet de redonner sens aux choix à faire pour des pratiques plus problématiques (comme transférer leurs données à des tiers qui n'ont rien à voir avec la finalité du traitement des données).
67. De nombreux répondants ont insisté sur le fait que le consentement doit être lié à la transparence. Pour Privacy International c'est même la transparence qui prime le consentement, dans le sens où il faut privilégier une information claire, facile à trouver et à comprendre à donner aux personnes concernées avant d'évaluer si on autorise un traitement (en se basant alors éventuellement sur un opt-out plutôt que sur un opt-in). Par ailleurs, d'autres contributeurs soulignent qu'il faut se méfier des *privacy policies* longues et rarement lues. Pour l'APEP-Association Professionnelle Espagnole de la Vie privée- on devrait introduire un devoir général d'information dans le but d'assurer la transparence.
68. La European Newspaper Publishers Association et la FAEP (European Federation of Magazine Publishers) signalent qu'une exemption pour les médias serait nécessaire pour toute question de consentement, que ce soit en termes d'obligation de transparence et

d'information ou comme une condition nécessaire à un traitement loyal et licite. Cela doit valoir pour toutes leurs activités : archivage d'articles, enregistrement de matériel de recherche pour préparer les articles, rassemblement quotidien d'informations, investigation, vérification, édition, suppression, que cela conduise ou non à la publication des matériaux, et enfin publication et communication ultérieure.

9. La Convention 108 devrait-elle aborder la question de la légitimation des traitements de données comme le fait la Directive 95/46 dans son article 7 ?

69. Certains contributeurs craignent que l'introduction d'une telle liste réduise la flexibilité de la Convention (TechAmerica). Le Garante, à l'instar du Commissioner for Personal Data Protection de Chypre et de CEA Insurers of Europe, souligne qu'il faut éviter de modeler de façon trop proche les principes de la Convention sur ceux établis dans la directive 95/46, ce qui conduirait à introduire des dispositions excessivement détaillées dans la Convention. Cette préoccupation est partagée par la German Insurance Association qui plaide pour un haut degré d'abstraction de la Convention, surtout en ayant en tête le souhait d'adhésion de pays tiers. Dans la même ligne, la FEDMA indique que cela ne devrait pas figurer dans le contenu d'une convention internationale. C'est davantage l'objet d'une directive.
70. Privacy International est plus radical encore. Ils estiment qu'une telle approche de la légitimité est tautologique et inutile. Ainsi, des finalités malhonnêtes sont de toute évidence non légitimes, à moins qu'elles le soient (sic) (hypothèse où l'on vise à tromper un escroc, par exemple). Pour eux, le catalogue des raisons de légitimation des traitements présent dans la directive a créé un terrain de jeu pour juristes plein de trous à éviter. Enfin, ils craignent qu'une liste de fondements positifs pour effectuer un traitement de données soit inévitablement incomplète. La combinaison de l'exigence de loyauté et licéité (« lawful (i.e. not unlawful) »), couplée aux autres principes généraux de proportionnalité, minimisation des données et collecte non intrusive, représente à leurs yeux des critères appropriés. Ces derniers points sont repris textuellement par le Cyberspace Law and Policy Centre et par le consortium CLSR-IAITL-ILAWS.
71. Aux antipodes, certains répondants trouvent opportun, utile voire important d'insérer une telle liste de fondements légitimes, par souci de cohérence avec le droit de l'UE ou par souci de clarté pour les acteurs de terrain qui ont besoin de disposer de paramètres clairs à propos des traitements licites (AEDH, European Privacy Association, European Banking Federation, Data Industry Platform, the CZECH Office for Personal Data Protection, la Commission pour la protection des données personnelles de Bulgarie, la Direcçao Geral da Politica de Justiça du Portugal, le Ministère de la Justice du Royaume-Uni). EFAMRO et ESOMAR accueillent favorablement l'introduction d'un fondement pour le traitement légitime des données dans la Convention mais ne sont pas en faveur d'une liste exhaustive de fondements légitimes.

10. La Convention 108 ne fait pas de référence expresse à la compatibilité nécessaire entre l'utilisation des données et le but initial de leur collecte. Or, aujourd'hui, les données à caractère personnel sont généralement utilisées à des fins qui vont bien au-delà de celles initialement prévues, d'où la question de la compatibilité.

72. Peu de répondants ont compris la pertinence de cette question étant donné que l'article 5 de la Convention exige déjà que les données ne soient pas utilisées de façon incompatible avec les finalités. Pour beaucoup la question est donc déjà réglée.
73. Certains notent toutefois que la question des traitements ultérieurs est de plus en plus fréquente, surtout dûe à la disponibilité massive des données sur le Net, et devrait être traitée.
74. Pour la European Privacy Association, la question principale n'est pas de mentionner l'exigence de compatibilité avec le but mais plutôt d'étendre l'application de l'article 5, b) de la Convention à tout traitement de données. Ils suggèrent de prendre pour modèle le texte de l'article 6, 1, b) de la directive.
75. Il est relevé qu'il faudrait permettre les traitements ultérieurs à des fins historiques, statistiques ou scientifiques. EFAMRO et ESOMAR demandent que la recherche de type « market, social and opinion research » ne soit pas considérée comme incompatible avec la finalité initiale d'un traitement de données, ce qui est déjà admis dans la recommandation R(97)18. Ces acteurs demandent qu'une disposition semblable à l'article 6, paragraphe 1.b) de la directive 95/46 soit intégrée dans la Convention.
76. CEA Insurers of Europe demande qu'il soit possible de changer de but, dans les cas où l'on peut justifier légalement le nouveau but.
77. Matthias Pocs, se penchant sur cette question au sein du secteur de la police où la question se pose avec acuité, propose, en étayant sa proposition de développements circonstanciés, que la Convention 108 prévoie que le traitement de données à caractère personnel pour des finalités différentes de celles spécifiées soit interdit si la personne concernée est suspectée d'une forme d'infraction peu grave ou modérément grave, mais qu'il soit autorisé si la personne concernée est suspectée d'une forme grave de crime et que des garanties adéquates contre les violations de la dignité humaine soient apportées.

11. La définition des catégories particulières de données faisant l'objet d'une protection accrue est très large, ce qui pourrait entraîner une application excessive de cette restriction : est-ce l'information ou son traitement qui est sensible ? Devrait-on ajouter d'autres catégories de données, comme les numéros d'identification (nationaux) et les données biologiques ou biométriques ?

78. **La pertinence d'une catégorie de données sensibles** : Le ministère de la justice britannique invite le Comité consultatif à réfléchir à ce que les données sensibles pourraient être liées à leur usage plutôt que simplement étendre la liste des données sensibles (il renvoie à l'exemple d'une photographie qui pourrait être considérée comme donnée biométrique et pour laquelle il y a une immense différence entre être reprise sur une carte de bibliothèque et être prise à la sortie d'un centre de désintoxication pour drogués). Cette position est partagée par plusieurs contributeurs pour qui la sensibilité des données est essentiellement contextuelle.

79. Pour plusieurs contributeurs, le principe de proportionnalité offre des garanties adéquates pour ces données. On pourrait ne pas toucher à la liste actuelle et reposer sur le principe de proportionnalité pour faire face aux dangers liés à d'autres données.

80. Pour le Garante italien, il ne faudrait pas toucher à la protection accrue offerte aux données figurant dans la liste actuelle, qui correspond grosso modo aux catégories protégées par les instruments internationaux pour lutter contre les discriminations. Par contre, on pourrait envisager un critère « fonctionnel » par lequel des catégories additionnelles de données pourraient être considérées comme sensibles à cause du contexte et/ou de la finalité et/ou des mécanismes de leur traitement. Dans ces cas, ces données seraient sujettes à une protection accrue. On pourrait également envisager que les circonstances et catégories de données puissent être déterminées et mises à jour régulièrement par des outils flexibles qui n'impliquent pas des amendements à la Convention. Cette position du Garante rejoint celle du Commissaire à la protection des données de l'Ile Maurice pour qui on pourrait distinguer les données sensibles du fait de leur nature et celles qui le sont du fait du traitement qui leur est appliqué (comme le nom ou la photo qui font apparaître l'origine raciale). L'APEP insiste aussi sur le fait que les dommages qui peuvent résulter du traitement de ces données sensibles dépend de la finalité du traitement.

81. **La liste des données sensibles** : plusieurs contributeurs s'interrogent sur ce que recouvre la notion de données « biologiques ». Pour certains cela ne devrait pas recouvrir des caractéristiques comme le genre et l'âge, visibles aux yeux de tout le monde.

82. Certains suggèrent l'introduction des données génétiques et biométriques dans la liste.

83. SAFRAN-groupe MORPHO, société spécialisée dans l'identification et dans les applications utilisant la biométrie, précise qu'à l'inverse du nom, les empreintes digitales ne donnent aucune indication sur l'origine ethnique ou sur l'appartenance à une religion supposée. Le nom est en outre la clé d'accès à des tas de données sur Internet par l'intermédiaire des moteurs de recherche, contrairement aux empreintes digitales. Cette société s'interroge donc : pourquoi soumettre les données biométriques à un régime juridique plus contraignant alors qu'elles fournissent moins d'informations que le nom des gens ? Par ailleurs, SAFRAN s'interroge sur le sort à réserver aux « empreintes vocales » récoltées par des systèmes de messagerie et stockées sur des serveurs pour constituer des bases de données biométriques. Ces données doivent-elles bénéficier d'un régime juridique différent des empreintes digitales et sur quel fondement ? Apportant encore des précisions sur les empreintes génétiques à distinguer des données génétiques, ce répondant signale que dans certaines situations l'utilisation de données biométriques comme l'iris ou l'empreinte digitale, anonymisées, permet de déterminer si un individu peut se voir ou non accorder un droit (d'entrer par exemple) sans que son identité ne soit dévoilée.

84. L'APEP-Association Professionnelle Espagnole de la Vie privée partage cette réticence à voir les données biométriques considérées comme sensibles, étant donné qu'en principe ces données ne révèlent pas d'informations sur la santé. Pour cet organisme, il est également difficile de considérer les numéros d'identification (nationaux) comme sensibles.

85. Pour l'AEDH, mises à part les informations biologiques nécessaires dans un contexte médical, il y a lieu de s'interroger si, au nom de la protection de la personne humaine, des informations telles que les identifiants nationaux et les données biologiques ou biométriques, qui servent donc d'identifiants sûrs d'une personne, devraient tout simplement exister, surtout quand elles concernent tous les membres d'un peuple et non certaines personnes pour des motifs particuliers au regard d'une nécessité publique. Pour cet organisme, l'existence de tels systèmes d'information est très dangereuse dans toutes circonstances exceptionnelles (régime devenant non démocratique). En outre, ces systèmes d'attachement physique des personnes à l'Etat rompt le contrat social et repose sur l'idée que tout citoyen est un délinquant potentiel, ce qui n'est pas acceptable. Ce n'est

donc pas un régime de protection renforcée pour prévenir les discriminations comme dans le cadre des données sensibles qui doit être réservé à de telles données. C'est un régime d'interdiction qui ne peut être levé que sur la base des critères énoncés à l'article 9 de la Convention.

86. La CNIL propose d'évoquer l'origine ethnique plutôt que l'origine raciale.
87. Plusieurs répondants demandent que si l'on songe à étendre la liste des données sensibles, cela soit précédé d'une étude d'impact.
88. Quant au **régime de ces données**, la CNIL demande qu'il soit plus détaillé car ce qui se trouve actuellement dans la Convention manque de précision. Cette autorité indique aussi qu'il faudrait une exemption pour les traitements statistiques et la recherche scientifique.
89. EFAMRO et ESOMAR souhaitent quant à eux que l'on apporte des clarifications sur la portée de ce qui constitue des données sensibles. Ils pointent également qu'imposer le recours à une autorité avant de permettre de traiter des données sensibles est une charge trop lourde et une entrave trop importante pour le secteur de la recherche.
90. La European Newspaper Publishers Association et la FAEP demandent une exemption pour le secteur de la presse par rapport au régime strict réservé aux données sensibles.

12. Une protection spécifique pourrait également être appliquée à certaines catégories de personnes sur lesquelles portent les données. Les enfants, en particulier, peuvent avoir besoin d'une protection spéciale en raison de leur vulnérabilité. Y-a-t-il un besoin de dispositions spécifiques à la protection des enfants ? Si tel est le cas, quels aspects devraient aborder ces dispositions ?

91. Les données relatives aux mineurs ne devraient pas tomber dans la catégorie des données sensibles étant donné que la personne concernée par les données ne peut être un critère de sensibilité (Commission pour la protection des données personnelles de Bulgarie).
92. Cela étant dit, il importe de prévoir des conditions particulières pour protéger les mineurs à cause de leur vulnérabilité. Cela semble nécessaire à plusieurs répondants. L'APEP-Association Professionnelle Espagnole de la Vie privée relève que tout le monde est d'accord pour dire que les enfants méritent une protection spécifique mais que le débat porte sur l'âge pertinent à prendre en considération, si et à partir de quand le contrôle parental porte atteinte au droit de l'enfant à la vie privée, qui doit octroyer l'autorisation parentale,… Pour cette association, des obligations spécifiques devaient être imposées dans les hypothèses où les enfants sont la cible du traitement. Le régime de protection spécifique devrait être basé sur des obligations de moyens et non de résultat.
93. La Federal Trade Commission présente le régime légal américain spécifique de protection des enfants en ligne (le Children's Online Privacy Protection Act) qui prévoit une série de règles visant à protéger les enfants de moins de 13 ans. Ce régime est en phase de révision pour s'assurer qu'il répond toujours adéquatement à l'évolution des technologies et surtout des pratiques qui a vu exploser l'usage des terminaux mobiles et des jeux interactifs par les enfants.
94. Par contre pour de nombreux autres, un régime de protection particulier n'a pas sa place dans la Convention. D'autres textes offrent un régime spécifique. Une recommandation serait sans doute plus appropriée en la matière. Ou, le rapport explicatif pourrait clarifier que l'introduction des principes de proportionnalité et de minimisation sont une réponse

adéquate aux préoccupations concernant les enfants – ainsi que d'autres groupes vulnérables (CLPC, Australie).

95. D'autant qu'il y a des difficultés à harmoniser ce qu'il faut entendre par mineur, mineur avec capacité de discernement et mineur avec capacité d'exprimer un consentement. De même qu'il y a des difficultés à faire respecter et contrôler des limites d'âge sur Internet.
96. Enfin, plusieurs contributeurs signalent qu'il y a d'autres catégories de personnes vulnérables que les mineurs.

13. L'article 7 de la Convention porte sur la sécurité des données au sens restrictif du terme, à savoir la protection contre la destruction accidentelle ou non autorisée, la perte accidentelle et l'accès non autorisé, la modification ou la diffusion. La notion de sécurité devrait-elle également inclure un droit pour les personnes concernées d'être informées des violations de la sécurité des données ?

97. Pour de nombreux répondants, il serait opportun de prévoir un tel droit à être informé des violations de sécurité, applicable de façon horizontale au sein de tous les secteurs. Pour le CLPC ainsi que pour le consortium CLSR-IAITL-ILAWS et pour Privacy International, ce droit ne devrait d'ailleurs pas paraître comme partie du principe de sécurité mais comme un principe séparé.
98. Il est impératif pour la plupart de baliser clairement les limites d'un tel droit. European Privacy Association précise qu'il faudrait indiquer quand l'information devrait être donnée, à qui et de quelle manière. TechAmerica Europe propose des balises pour définir cette obligation. La Commission à la protection des données du Sénégal estime qu'il faut obliger à informer les autorités publiques de contrôle mais non les personnes concernées qui ne pourront de toute manière rien faire face aux violations. La German Insurance Association apporte l'éclairage de l'expérience allemande : en 2009, un amendement de la législation allemande de protection des données a introduit un devoir d'informer en cas d'accès non autorisé aux données. Cette obligation s'applique si des données particulièrement sensibles sont affectées et s'il y a un risque réel d'atteinte sévère aux droits ou aux intérêts légitimes des personnes concernées. A leur connaissance cette règle a suscité une expérience positive. Ils insistent sur la nécessité de limiter ce genre d'obligation aux seuls cas de risque réel pour les personnes concernées. Morpho-groupe Safran ne se penche pas sur les hypothèses d'accès non autorisés mais estime que ce droit à être informé des violations de sécurité devrait être expressément justifié par la nécessité de protéger l'identité et de limiter les risques d'usurpation d'identité.
99. Toutefois, plusieurs répondants craignent qu'il ne soit pas possible d'introduire un tel droit sous peine de transformer la Convention en instrument trop détaillé et non restreint à des principes généraux.

100. Certains répondants, comme l'Office de protection des données personnelles de la République tchèque, sont opposés à l'idée d'introduire ce droit estimant que la question est suffisamment traitée au sein de la directive européenne. La Data Industry Platform craint qu'on n'impose des charges additionnelles sur les acteurs de terrain sans apporter aux personnes concernées un plus haut niveau de protection. Ce groupe de signataires comprend l'importance de la sécurité et de la nécessité de créer la confiance entre les personnes concernées et les responsables de traitement. Ils trouvent donc le concept « sympathique » dans la mesure où c'est un incitant à la sécurité. Ils estiment toutefois que la question serait plus adéquatement adressée par des instruments d'autorégulation. La FEDMA et la European Banking Federation ont formulé exactement les mêmes craintes et convictions. EMOTA (European E-commerce and Mail Order Trade Association) partage également ces doutes.

101. Plusieurs ont indiqué qu'il ne fallait en tout cas pas tomber dans une formule « *overly prescriptive* » qui conduirait à une charge excessive et enlèverait en même temps son efficacité à la mesure, banalisant les notifications auprès des intéressés.

102. Pour le Garante italien la question de la sécurité est devenue une question cruciale, surtout dans le contexte du *cloud computing*. L'article 7 de la Convention devrait être revu. Il serait approprié d'envisager d'étendre le concept de sécurité pour inclure la sécurité des réseaux de transmission de données en sus de la sécurité physique des locaux où les données sont conservées.

103. Dans le même sens, Privacy International recommande que l'on passe d'une « sécurité des données » interprétée passivement à une obligation positive de concevoir les systèmes pour minimiser le risque pour la vie privée – par exemple par une minimisation ex ante. Il ne faut donc pas seulement veiller à protéger les données qui sont traitées mais à minimiser le risque pour la vie privée du système tout entier.

14. Il existe certains risques découlant de l'utilisation des données de trafic et de localisation (données techniques accompagnant une communication) car ces données peuvent révéler les mouvements, orientations, préférences et associations avec d'autres. Avons-nous besoin de règles particulières pour l'utilisation de ce type de données ?

104. Les réponses à cette question sont contrastées.

105. Certains estiment que ce serait opportun de prévoir un régime de protection renforcée pour les traitements visant à localiser les individus dans l'espace.

106. L'AEDH précise que les données de trafic mettent en jeu la liberté de communication, et les données de localisation la liberté d'aller et venir. De par cette interférence sur des libertés, un régime plus strict devrait leur être appliqué. Il en est de même pour les requêtes formulées sur un moteur de recherche qui mettent en jeu la liberté d'information. Dans le même sens, pour Privacy International, les données de trafic et de localisation sont des données concernant les relations sociales et empiètent sur la liberté d'association et sur le droit de s'associer librement de manière privée et non observée. En conséquence, pour Privacy International, de telles données doivent constituer une catégorie spéciale et devraient être considérées comme intrinsèquement « toxiques » pour la vie privée.

107. La CNIL signale que faire entrer ces données dans la catégorie des données sensibles risque de conduire à placer un frein à certaines innovations techniques. Il serait préférable plutôt d'ajouter des éléments de protection clairement distincts dans la Convention visant notamment à imposer des garanties appropriées pour « les données à caractère personnel utilisées dans des traitements ayant pour finalité de révéler la position dans l'espace d'un individu ». Cela permettrait d'exclure les données qui peuvent révéler la localisation d'un individu mais dont ce n'est pas la finalité tout en ne faisant pas entrer ces données dans les données spéciales visées à l'article 6 de la Convention. Une troisième option possible présentée par la CNIL serait de proposer un droit spécifique à ne pas être géo-localisé.

108. Pour d'autres répondants, il n'est pas nécessaire de prévoir un régime spécifique. L'Information Commissioner britannique, pour sa part et dans le même sens, estime que la sensibilité tient davantage dans le traitement des données et les effets qu'il peut avoir sur les individus que dans la nature des données traitées.

109. Pour le CLPC, appuyé par le CIPPIC, il ne devrait pas y avoir besoin d'un régime particulier si l'on veille à faire entrer les données de trafic et de localisation dans la définition des données à caractère personnel en prévoyant expressément que les données à caractère personnel englobent toute information qui permet ou facilite la communication avec une personne sur une base individualisée, que cette information rencontre ou non l'actuelle définition de donnée à caractère personnel.

15. Faut-il mettre en place des systèmes de responsabilisation, ainsi qu'une obligation de prouver que des mesures efficaces ont été prises pour garantir le plein respect de la protection des données ?

110. La plupart des répondants qui se sont prononcés sur cette question approuvent l'idée d'introduire une obligation de respect du principe « d'*accountability* », comme garantie d'amélioration de la protection offerte. Les mécanismes d'*accountability* devraient être clairement définis, non excessifs et mis en œuvre de la même façon parmi les signataires.

111. Privacy International, de même que le consortium CLSR-IAITL-ILAWS, invitent à se montrer prudent par rapport à la suggestion faites par certains de voir l'*accountability* comme une alternative à l'exigence de respect des règles de protection. L'*accountability* ne peut devenir une alternative aux restrictions d'exportation de données. Cette organisation est préoccupée à propos des conséquences ou plutôt de l'absence de conséquences que des failles au niveau de l'*accountability* peuvent avoir si ce principe est interprété de façon laxiste.

112. L'APEP-Association Professionnelle Espagnole de la Vie privée estime pour sa part qu'il faudrait octroyer une « récompense » (une réduction de sanction, par exemple) pour les responsables de traitements « *accountable* » dans les hypothèses où les violations de la protection des données sont dues seulement à une erreur exceptionnelle.

113. TechAmerica Europe soutient l'introduction d'un principe d'accountability s'il est défini dans une approche ex post basée sur l'application des règles plutôt que dans une approche ex ante basée sur la conformité aux règles. Dans un régime ex post, les organisations sont responsables de ce qu'elles font avec les données où que celles-ci aillent, au lieu de chercher simplement à être en règle avec la loi. Cela a

des implications sur comment l'organisation considère la protection des données, comment elle la met en œuvre et comment elle la supervise.

114. Certains répondants s'opposent à l'idée d'introduire une obligation de démontrer la conformité car cela représenterait une charge, spécialement pour les PME.

16. Devrait-on appliquer le principe du « respect de la vie privée dès la conception » (Privacy by Design) qui vise à prendre en compte la question de la protection des données dès le stade de la conception d'un produit, d'un service ou d'un système d'information ?

115. Il semble cohérent, au vu du fait que le principe de *Privacy by design* a été proclamé dans différentes enceintes, a fait l'objet d'une résolution adoptée par la 32eme conférence internationale des autorités de protection des données et est pris en considération par la Commission européenne dans le cadre de la révision de la directive 95/46, que ce principe soit également consacré par la Convention 108 (SAFRAN).

116. D'autres répondants partagent la conviction que ce principe devrait être expressément encouragé, même s'il sera difficile de l'opérationnaliser en une règle spécifique (Privacy International, Ministère de la Justice britannique, CNIL, Commission à la protection des données du Sénégal). Ou qu'il est bienvenu mais qu'il faudrait clarifier bien davantage comment il sera défini ou mis en œuvre avant de pouvoir véritablement le soutenir (TechAmericaEurope). L'introduction du principe de *Privacy by design* favoriserait une approche proactive de la protection plutôt que de reposer exclusivement sur des mesures de redressement (Garante). Pour l'AEDH, l'obligation d'appliquer les principes de protection dès la conception des équipements et des applications pourrait être simplement précisée dans le texte, sans forcément recourir à une « vocabulaire marketing » tel celui de *privacy by design*. Pour le ICUK, ce principe se trouve implicitement dans les principes de protection existants. Toutefois, une exigence explicite aurait l'avantage de donner un signal clair aux concepteurs de systèmes d'information, à ceux qui les approvisionnent et à ceux qui les font fonctionner.

117. Le Garante italien précise toutefois que l'efficacité du principe ne pourra être assurée qu'en spécifiant comment son impact sur les opérations spécifiques du traitement peut ou devrait être mesuré et par qui, à la lumière de dispositions technologiques spécifiques.

118. La Commission pour la protection des données personnelles de Bulgarie estime que pour une application effective de ce principe il faudrait prévoir l'obligation pour les responsables de traitement d'effectuer des évaluations de risque pour la vie privée lors du traitement de données. Privacy International est également favorable à une obligation d'effectuer des « privacy impact assessment » pour les projets majeurs.

119. Pour cette dernière organisation, le moyen le plus simple d'exprimer le principe de *privacy by design* consiste à dire que si des découvertes scientifiques démontrent qu'un service peut être offert pratiquement par une voie plus respectueuse de la vie privée, l'adoption de technologies protectrices de pointe peut être imposée. Ils relèvent encore qu'il ne faut pas être influencé par la fausse rhétorique des lobbyistes qui tentent de cantonner la *privacy by design* à un simple état d'esprit attentif aux principes de protection des données lors de la conception des produits commerciaux, « immunisant » le concept de toutes obligations techniques.

120. Pour TechAmerica Europe, la *privacy by design* est un processus que les organisations devraient suivre au début d'un projet et réévaluer régulièrement pour assurer que les mesures de protection des données et de sécurité demeurent appropriées. Il est important que quelle que soit l'exigence introduite dans le texte légal, cela reste de l'ordre des procédures et non de la technologie. Pour AFME BBA (monde bancaire), la formulation du principe doit être de haut niveau et non prescriptive quant aux mesures qui devraient être adoptées.

121. La FTC a pour sa part recommandé dans son rapport destiné à améliorer la protection de la vie privée aux Etats-Unis que les entreprises adoptent une approche « *privacy by design* ». Ceci implique de construire des protections pour la vie privée au sein des pratiques journalières des affaires. Ces protections incluent l'offre d'une sécurité raisonnable pour les données à caractère personnel, la limitation de la collecte de données aux seules données nécessaires et la conservation des données durant une période limitée. Sur la base de son expérience, la FTC encourage le Comité consultatif de la Convention 108 à retenir le concept d'adaptabilité en abordant la question de *privacy by design*.

Droits – Obligations

17. Le droit d'accès ne devrait pas se limiter aux données mais devrait couvrir l'accès à l'origine des données, c'est-à-dire la personne qui est à l'origine de la communication. Ce droit devrait-il également couvrir l'accès à la logique du traitement ?

122. L'ajout du droit d'accès à l'origine des données et à la logique qui sous-tend un traitement est absolument nécessaire aux yeux de l'AEDH, très importante, pour la Commission bulgare, permet la cohérence avec le régime de l'UE, pour le ICUK et le Ministry of Justice britannique, s'impose dans le contexte grandissant des modèles informatiques complexes sur lesquels on base des critères et des suppositions et qui peuvent avoir un effet négatif sur la sphère privée des individus, pour le CIPPIC et le Garante, et doit tout simplement être envisagé pour d'autres répondants. La European Privacy Association craint toutefois qu'étant donnée l'implication d'un nombre important d'intervenants dans les traitements automatisés aujourd'hui, l'obligation de transparence du processus de traitement – que cette association soutient – ne soit plus réalisable sans supporter des coûts excessifs.

123. L'AFME et BBA (banques) soutient l'initiative pourvu que cela ne dépasse pas le droit instauré par la directive 95/46, dans la mesure où cela ne reviendrait pas à obliger les acteurs à conserver des informations sur les sources des données, mais ne représente qu'un devoir de transmettre les informations sur les sources si celles-ci sont connues. Sur le point de la conservation des informations sur les sources des données, la réponse de la German Insurance Association indique que la loi allemande de protection des données impose l'obligation de conserver les données sur les sources et sur les destinataires des données durant une période de deux ans.

124. La Direcçao Geral da Politica de Justiça du Portugal estime que l'accès à la logique du traitement nécessite pour le sujet des données de démontrer un intérêt et doit être limité dans la mesure stricte de la satisfaction de cet intérêt. L'accès à la logique du traitement ne doit donc pas se traduire en divulgation injustifiée de secrets d'affaires.

125. CEA Insurers of Europe relève que certaines demandes d'accès sont « frivoles » et ne visent qu'à contrôler le traitement de données plutôt qu'à vérifier l'exactitude des données traitées. En conséquence ce groupe estime que le droit d'accès devrait être limité et qu'on ne devrait pas envisager d'introduire le droit d'accès à connaître la logique dans la Convention108. Cette position est partagée par la Data Industry Platform qui est soucieuse de préserver les secrets commerciaux, la compétitivité des entreprises et leur propriété intellectuelle. Les techniques internes d'analyse prédictive sont une valeur cruciale pour le monde des affaires et ne devraient pas être révélées à des tiers. La FEDMA rejoint cette position.

126. Privacy International estime que la protection offerte à la propriété intellectuelle (brevets) permet d'être transparent sans crainte. Dans les cas exceptionnels où le secret doit être préservé, il faudrait que les autorités de contrôle puissent inspecter confidentiellement les algorithmes pour en vérifier la légitimité.

127. La FTC fournit des indications de cas dans lesquels aux Etats-Unis les consommateurs ont le droit d'obtenir des informations des entreprises qui ont pris des actions ayant un effet négatif sur eux. Un cas illustre que l'on peut atteindre un compromis entre transparence et secret des affaires : les agences de credit reporting ne sont pas tenues de révéler précisément comment les scores de crédit sont calculés, mais la divulgation qu'elles doivent effectuer doit inclure l'éventail des scores de crédits possibles dans le modèle d'évaluation et les facteurs clés qui ont affecté négativement le score du consommateur.

128. La CNIL insiste pour que l'exercice des droits d'accès, d'opposition, de correction et blocage se fasse gratuitement.

129. Le Garante invite à réfléchir, concernant les technologies basées sur le cloud computing, à introduire un droit de connaître la localisation physique et le pays où la conservation des données ou les serveurs de distribution sont situés.

18. Le droit d'opposition se justifie dans les cas où le traitement des données ne repose pas sur le consentement de la personne concernée. Le lien entre droit d'opposition et droit à l'oubli pourrait être examiné, ainsi que la possibilité de garantir le respect et l'exercice de ce droit.

Le droit d'opposition

130. Le droit d'opposition se justifie aux yeux de la plupart des répondants, mais pas en toutes circonstances. On pourrait songer à introduire ce droit dans la Convention par souci de cohérence avec la directive. A l'inverse de certains répondants, d'autres estiment que ce droit devrait être accordé même lorsque le traitement se fonde sur le consentement, s'il est admissible que le consentement soit révocable en toutes circonstances.

131. Un droit proche existe dans la loi canadienne (PIPEDA), permettant aux personnes concernées de s'opposer par opt-out aux finalités non nécessaires pour la collecte, l'utilisation et la communication des données à caractère personnel.

132. La Commission bulgare a souligné que le lien entre le droit d'opposition et le droit à l'oubli consiste en ce que le droit d'opposition s'exerce en tenant compte de la finalité du traitement, tandis que le droit à l'oubli s'exerce au-delà de la question d'une justification du traitement au regard de la finalité.

Le droit à l'oubli

133. Il ressort de la plupart des réponses ce qui suit. Le droit à l'oubli peut être particulièrement indiqué et praticable dans certaines circonstances (essentiellement dans le cadre des réseaux sociaux). Pour le reste, il est problématique sur plusieurs points :

134. - il entre en conflit avec les droits, intérêts et libertés d'autrui, notamment la liberté d'expression, la liberté de la presse (il empiète sur la conservation d'archives complètes), le devoir de mémoire, la continuité des affaires, la gestion des dossiers des employés, le devoir de conserver les preuves… Il est une entrave à la recherche historique. Il peut également entraver la fourniture de certains services comme les soins médicaux au cas où il n'y a plus connaissance du passé médical de la personne concernée ;

135. - il est difficile à mettre en œuvre une fois que les données ont été rendues publiques sur internet.

136. Pour l'APEP, le droit à l'oubli n'est pas une sous-catégorie du droit d'opposition dans la mesure où, à la différence de ce dernier, il a un effet rétroactif. La question est donc, pour cet organisme, de savoir si les individus doivent être responsables sine die de leurs actions passées et s'il est souhaitable qu'ils aient le droit de réécrire leur passé, et donc aussi le passé des autres.

137. Certains répondants soutiennent son insertion dans la Convention. D'autres, plus nombreux, estiment qu'il faut approfondir la réflexion avant de se prononcer, notamment en se penchant sur les obstacles pratiques à sa réalisation et en éclaircissant le coût et les implications concrètes induits par un tel droit. Des éclaircissements sur les données qui seraient l'objet d'un tel droit d'effacement devraient aussi être apportés : si cela concerne les données provenant de la personne concernée, cela couvre-t-il aussi les données d'analyse ou méta-données créées par le responsable du traitement ? On souligne que le droit à l'oubli ne peut en tout cas pas être absolu. La Data Industry Platform relève que ce droit ne devrait pas figurer dans un catalogue de principes généraux et éprouvés dans la durée. Sur ce point elle est appuyée par le Garante qui ne voit pas d'un bon œil l'insertion d'un droit aussi controversé dans la Convention.

138. Pour la Data Industry Platform, si l'on devait envisager l'insertion de ce droit, il faudrait impérativement le limiter aux services basés sur des données que les individus concernés ont eux-mêmes fournies et qui sont rendues accessibles à des tiers comme objet du service. Certains répondants rejoignent cette position, limitant le champ d'application d'un tel droit aux réseaux sociaux.

139. Pour d'autres répondants, enfin, ce droit est carrément irréaliste sur les plans technique et légal (EMOTA- European E-commerce and Mail Order Trade Association) ou aurait des conséquences désastreuses pour les éditeurs et la liberté d'expression (European Newspaper Publishers Association et European Federation of Magazine Publishers) et devrait absolument être rejeté (notamment les différents intervenants du monde de la presse).

19. Devrait-il y avoir un droit qui garantisse la confidentialité et l'intégrité des systèmes d'information ?

140. Il est à noter que d'assez nombreux répondants ont omis de répondre à cette question.

141. Pour certains répondants la réponse est positive, la plupart du temps non étayée. Parmi ceux-ci, le Garante italien se démarque en exprimant que, pour lui, les droits en cause à cette question, de même que ceux en jeu dans les deux questions suivantes, sont ceux qui justifient le plus d'étendre la liste des droits et des principes généraux de la Convention.

142. Mais d'autres répondants ne voient pas en quoi la confidentialité et l'intégrité des systèmes devraient faire l'objet d'un droit, plutôt que de renforcer les contraintes de sécurité de l'article 7. La plus-value d'un tel droit resterait à démontrer et devrait être confrontée au risque de dilution et de perte de lisibilité des droits figurant dans la Convention.

143. L'Office pour la protection des données personnelles tchèque précise que la garantie de confidentialité se rattache aux obligations pesant sur le responsable et non aux droits.

20. Faudrait-il introduire le droit de tout individu à « ne pas être localisé / tracé» (identification RFID) ?

144. Certains répondants sont d'accord à l'idée d'introduire un tel droit, mais avec des exceptions raisonnables.

145. Rappelons la remarque du Garante formulée à propos des trois droits en cause aux questions 19, 20 et 21, qui estime ce droit crucial.

146. Pour d'autres, ce droit nécessite une réflexion plus approfondie.

147. L'AEDH et la Data Industry Platform pensent que l'application des principes généraux de protection (notamment l'interdiction de conservation des données au-delà de l'objectif) offre une réponse satisfaisante. Le CIPPIC, dans le même sens, estime que les principes « de confidentialité, de vie privée et d'exactitude » réalisent ce droit. Le CLPC, quant à lui, estime également qu'il n'y a pas besoin de consacrer un droit séparé si l'on définit les données à caractère personnel de manière à englober les informations à propos des communications, de la localisation ou du comportement d'un individu.

148. European Privacy Association suggère que plutôt que de parler d'un droit à ne pas être tracé, on mette en place une option à ne pas être tracé. Les personnes concernées devraient être informées des pratiques de traçage et se voir fournir l'option et les moyens technologiques de refuser d'être tracé/localisé. L'APEP parle également d'une option à rendre disponible aux personnes concernées, refusant l'idée d'une interdiction. Les technologies de traçages ne sont pas mauvaises en soi mais certains usages doivent être limités dans les cas où la vie privée doit l'emporter. Pour cet organisme on ne devrait pas empêcher le traçage des patients Alzheimer, des bagages perdus, des véhicules, des enfants ou des animaux. Par ailleurs le concept de traçage n'est pas limité au RFID mais couvre aussi notamment les cookies.

149. Plusieurs répondants font remarquer qu'il ne faut pas baser un droit sur une technologie ciblée, cela est contraire à l'objectif de conserver à la Convention son caractère technologiquement neutre.

150. Il ne faut pas non plus que par la législation on empêche tout progrès et tout développement technique en la matière.

21. Les utilisateurs des technologies de l'information et de la communication devraient-ils avoir le droit de rester anonymes ?

151. Rappelons la remarque du Garante formulée à propos des trois droits en cause aux questions 19, 20 et 21, qui estime ce droit crucial.

152. L'AEDH relève que la vie sociale repose sur une dialectique de l'identification et de l'anonymat qui ne se retrouve plus dans les conditions d'aujourd'hui où par exemple, la consultation d'informations publiques laisse des traces identifiantes de même que tout paiement puisqu'il n'y a pas de monnaie électronique équivalant aux billets de banque. Cela constitue un « vice de base ». Tout repose dans un tel contexte sur la durée de conservation des données collectées. Il faudrait, aux yeux de cette association, garantir socialement et techniquement un droit à l'anonymat.

153. Dans la même ligne, le CIPPIC est d'avis que l'anonymat est un droit qui mérite une formulation et une protection distinctes. Pour ce centre, la capacité d'agir anonymement est centrale dans la protection de la vie privée dans les espaces publics et semi publics. Il signale que la formulation du principe qui est proposée par le CLPC sur la base de ce qui se trouve dans la législation australienne de vie privée est intéressante. Le CLPC propose la formule suivante : « Les individus doivent avoir l'option de ne pas s'identifier lorsqu'ils traitent avec une entité, ou d'utiliser un pseudonyme, excepté en présence d'une obligation légale d'identification ou s'il est impraticable pour l'entité de traiter avec des individus qui ne se sont pas identifiés ou qui utilisent un pseudonyme. ».

154. Plusieurs répondants sont favorables à un droit à l'anonymat tant que l'on ne viole pas la légalité.

155. Pour plusieurs commentateurs, par contre, il ne devrait pas y avoir un droit à l'anonymat car cela pourrait conduire à une augmentation de la fraude et de la criminalité, rendant difficile voire impossible la recherche des auteurs. La European Privacy Association s'oppose à un droit générique à être absolument anonyme lorsqu'on utilise les TIC, qui serait contraire aux nécessités pratiques (les citoyens ont besoin d'information sur leur utilisation des TIC, à tout le moins pour l'établissement de factures liées à cette utilisation) et aux besoins des services de lutte contre la criminalité. Par contre ces informations doivent être protégées contre les usages abusifs. Pour la EPA, cette protection est déjà assurée par la Convention. L'APEP donne l'exemple de la surveillance légitime par le patron des actions de ses employés dont il sera rendu redevable.

156. La Data Industry Platform, à l'opposé de ce qui a été relevé ci-dessus, demande si le monde hors ligne connaît vraiment des mécanismes par défaut ou un droit de demeurer anonyme dans les circonstances normales de la vie. Ainsi, le personnel d'une bibliothèque publique connaît les utilisateurs de cette bibliothèque ainsi que leurs préférences de lecture… Ce groupe ne voit aucune raison pour faire une distinction entre le monde en ligne et le monde hors ligne.

22. La Convention 108 devrait-elle aborder la question du juste équilibre entre la protection des données à caractère personnel et la liberté d'expression (nouveau concept de la presse et du journalisme dans le contexte du Web 2.0.) ?

157. Oui en général mais les répondants sont nuancés sur la manière.

158. Pour la European Privacy Association, il conviendrait d'établir le lien existant entre le droit à la protection des données et la liberté d'expression, lien décisif. Un lien avec l'article 10 CEDH pourrait être abordé dans les considérants de la Convention 108.

159. Pour l'Union européenne de Radio-Télévision (EBU-UER), l'article 9, 2, b) accompagné du point 58 du rapport explicatif n'est pas suffisant et devrait être explicitement renforcé pour donner une exemption claire de l'application de certaines règles de protection des données pour les activités de journalisme, en particulier dans le champ audiovisuel. Cet organisme propose en conséquence d'amender l'article 9 en ajoutant un alinéa qui stipule : « 9, 2, c) protéger le traitement de données à caractère personnel effectué exclusivement à des fins journalistiques ». Une telle modification est vitale aux yeux de l'UER afin de préserver la liberté des médias, le journalisme d'investigation et la confidentialité des sources journalistiques.

160. Le Centre for Socio-Legal Studies propose quant à lui de rédiger une nouvelle disposition qui enjoint les Parties signataires de présenter un équilibre entre l'intérêt fondamental de la liberté d'expression et les valeurs que la protection des données tend à protéger. La disposition devrait en outre indiquer la nécessité d'adopter des exemptions larges, mais non absolues, des règles de protection au bénéfice de ces activités. Quant à la possibilité d'indiquer expressément les exemptions minimum en conformité avec l'article 10 CEDH, elle nécessite d'être davantage creusée. Le rapport explicatif devrait signaler explicitement que cette disposition protégeant la liberté d'expression n'est pas limitée à la presse. En principe cette disposition devrait valoir pour toute forme d'expression publique.

161. Pour l'APEP, toute régulation dans cette matière requiert de la flexibilité : elle ne doit apporter que des critères d'orientation mais pas effectuer elle-même une évaluation générale prédéterminée. Tandis que pour la CNIL, des dispositions similaires à celles de la loi française Informatique et Libertés pourraient être intégrées dans la Convention. Cet organisme trouverait en effet utile de préciser au plan européen les exemptions et dérogations dont les traitements pourraient bénéficier. Pour le CLPC, il ne serait pas approprié que la Convention fasse elle-même la mise en balance de tous les aspects de ces intérêts contradictoires, mais elle devrait néanmoins contenir une reconnaissance de l'intérêt public de la liberté d'expression.

162. L'AEDH relève qu'il n'y a pas de consensus même en Europe sur les limites à apporter à la liberté d'expression au nom de la protection de la vie privée. Cette association prône donc une initiative visant au rapprochement des points de vue et des procédures. Cette initiative devrait être prise au sein du Conseil de l'Europe, éventuellement en relation avec l'UNESCO.

163. Le ICUK s'interroge : à l'ère du blogging, où faudrait-il tracer la ligne ? Jusqu'où les autorités de contrôle seront-elles amenées à réguler le comportement en ligne des individus ?

164. Le Garante italien est opposé, pour sa part, à ce qu'on intègre dans la Convention des dispositions qui pourraient s'avérer moins flexibles que ce qui ressort du travail jurisprudentiel effectué par la Cour européenne des droits de l'homme pour réconcilier les deux droits ou qui n'atteindraient pas le même équilibre. Pour ce qui concerne les questions liées spécifiquement au Web 2.0, il lui semble prématuré d'édicter des règles spécifiques.

Sanctions et recours

23. Devrait-on introduire des recours collectifs dans la Convention ? Faut-il examiner l'introduction d'autres mécanismes de règlement des litiges ?

165. **Recours collectifs**. Différents répondants à la consultation jugent que l'introduction de la « class action » paraît souhaitable, soit dans certains contextes spécifiques[5], soit de manière générale et qu'il en soit question, le cas échéant, dans la Convention[6]. D'autres relèvent au contraire que la généralité de la Convention ne s'y prête pas[7]. Dans le même sens, plus largement, la question des sanctions et remède devrait plutôt relever du droit national que de la Convention[8]. Certains évoquent par ailleurs que le débat relatif à la « class action » doit avoir lieu dans un contexte plus large que celui de la protection des données[9].

166. Outre ces oppositions de méthodes apparaissent certaines réticences vis-à-vis de l'introduction générale des « class actions ». Des répondants notent qu'il n'en est pas besoin[10], voire même que ce n'est pas approprié[11]. Les « class actions » n'auraient pas d'intérêt lorsque la personne concernée peut déjà bénéficier de mécanismes protecteurs la soutenant dans l'exercice de ses droits[12] (par ex., les autorités de protection des données). Le recours collectif ne serait alors utile que lorsque les autres recours sont fébriles[13], inefficaces, bref quand il y aurait un

[5] Avis CIPPIC.

[6] Avis Czech Republic – The office for personal data protection; avis Ile Maurice-Commissariat à la protection des données; avis Ukraine-Ministry of justice ; avis United Kingdom-Information commissioner's office ; avis Direcção-General da Politica de Justica.

[7] Avis EPA ; avis Italy-Garante per la protezione dei dati personali. Différents intervenants soulignent qu'il s'agit d'une question de droit national, voy. par exemple avis Lithuania-State data protection inspectorate.

[8] Avis CEA.

[9] Avis EBF.

[10] Avis Data Industry Platform.

[11] Avis ENPA-FAEP.

[12] Avis German Insurance Association ; voy. aussi avis Techamerica Europe, où il est souligné en outre qu'il faudrait évaluer s'il y a une demande des citoyens en ce sens.

[13] Avis Italy-Garante per la protezione dei dati personali.

véritable intérêt concret à recourir à ce moyen[14]. D'autres relèvent que les litiges en matière de protection des données seraient propres aux individus et se prêteraient par conséquent mal au recours collectif[15]. D'autres répondants encore soulignent le risque de l'utilisation nuisible des règles de protection des données que permettraient les recours collectifs[16]. Traiter à ce stade des recours collectifs serait également source d'incertitude[17].

167. Quoi qu'il en soit, la Convention pourrait néanmoins souligner l'intérêt des « class actions », leur valeur, si elle traitait finalement de la question des voies de recours[18]. Et si l'on envisageait de recourir aux recours collectifs, il importerait avant tout d'évaluer l'impact qu'ils pourraient avoir dans le contexte européen[19].

168. **ADR**. Des répondants manifestent leur soutien au recours à des ADR[20], vus par certains comme rapides et peu chers[21]. Dans le même sens, il est parfois insisté sur l'importance que pourrait recouvrir l'autorégulation dans un régime moderne de protection des données[22]. Certains répondants soulignent que la question de la résolution des litiges par des modes alternatifs est une question qui doit toutefois être réglée par les Etats et pas dans la Convention[23]. Ce serait en outre une question qui devrait être discutée dans le contexte de l'Union européenne[24]. On pourrait imaginer que la Convention se limite à consacrer l'obligation de créer des moyens alternatifs de règlement des différends mais que la matière demeurerait réservée au droit interne[25].

169. Différents intervenants notent que s'il est décidé de recourir aux ADR, cela ne devrait en tous cas pas limiter les autres voies de recours disponibles aux personnes concernées[26]. Le recours à l'ADR ne devrait pas, en outre, être une étape obligatoire et préalable à tout recours judiciaire – ou autre mais néanmoins impliquant l'autorité publique –, comme il ne pourrait constituer le seul moyen de résolution des litiges offert aux personnes concernées[27]. En cas de recours aux

[14] Avis UK Ministry of Justice.

[15] Avis FEDMA.

[16] Avis APEP.

[17] Avis EMOTA.

[18] Avis Cyberspace Law and Policy Centre ; avis CLSR-IAITL-ILAWS ; avis Privacy International.

[19] Avis CNIL ; avis UK Ministry of Justice.

[20] Avis FEDMA ; avis United Kingdom-Information commissioner's office ; avis UK Ministry of Justice .

[21] Avis FEDMA .

[22] Avis United Kingdom-Information commissioner's office .

[23] Avis commun de l'AFME et de la BBA .

[24] Avis CEA.

[25] Avis Direcção-General da Politica de Justica.

[26] Avis CIPPIC.

[27] Avis CNIL.

ADR, il serait par exemple recommandable d'utiliser les organes d'arbitrages déjà existant pour l'application de la protection des données[28].

170. Plusieurs répondants relèvent l'importance du rôle que peuvent jouer les **autorités de protection des données** – les « *Data Protection Officers* » inclus – en matière de règlement des différends. Ainsi, certains considèrent qu'elles peuvent être chargées de traiter la résolution de litiges[29]. Elles ont à cet égard besoin de la liberté d'établir des procédures et la Convention pourrait fixer un cadre normatif à cette fin[30]. En ce sens, il serait par exemple opportun de donner aux autorités de protection des données le pouvoir d'agir *ex officio*[31]. Elles pourraient également avoir la possibilité d'intervenir librement devant les juridictions judiciaires et administratives lors d'instances en cours[32].

171. **Autres.** Dans un tout autre ordre d'idées, certains insistent sur l'utilité de créer des **incitants** au respect de la protection des données (par ex., une réduction graduelle des exigences administratives basées sur l'historique de l'entreprise en matière de simple respect de la protection des données, voire de surpassement des exigences normalement requises)[33].

Droit applicable en matière de protection des données

24. Doit-on envisager une règle qui déterminerait le droit applicable au traitement des données (dans les cas où différentes juridictions sont concernées) ?

172. **Généralités**. Le problème du droit applicable apparaît comme important pour de nombreux répondants recommandant à plusieurs reprises que les règles soient clarifiées, en particulier dans le contexte du « Cloud Computing » (exemple fréquemment cité). La problématique du droit applicable est parfois considérée comme un obstacle pour des organisations non basée dans l'Union européenne souhaitant y établir des opérations de traitement ; le droit européen s'appliquerait sans que cette application ne soit justifiée par un lien assez fort entre la situation des individus et le droit de l'Union[34]. Certains répondent pourtant qu'ils sont

[28] Avis German Insurance Association.

[29] Avis GDD ; avis United Kingdom-Information commissioner's office.

[30] Avis United Kingdom-Information commissioner's office

[31] Avis German Insurance Association

[32] Avis CNIL

[33] GS1 in Europe.

[34] Avis commun de l'AFME et de la BBA.

convaincus que les règles actuelles en matière de définition du droit applicable sont efficaces[35].

173. Le risque qui existe en la matière est classique en droit international privé : soit il risque d'y avoir une lacune dans la protection (aucun droit applicable), soit il pourrait y avoir cumul des réglementations applicables[36]. Deux tendances concordantes en ce qu'elles souhaitent plus d'harmonisation se présentent auprès des sondés : plus d'harmonisation des concepts et règles de fond est souhaitée, et plus de clarté est demandée quant à la détermination du droit applicable. Quant à ce dernier point, les répondants émettent diverses suggestions.

174. **Harmonisation des règles de fond.** Il est clair que l'harmonisation des réglementations nationales et une interprétation conforme de la Convention auraient un effet positif[37] dans la mesure où la question du droit applicable – pour peu qu'il soit celui d'un des Etats membres du Conseil de l'Europe – perdrait de son importance – les droits étant harmonisés. En ce sens, certains soulignent la possibilité d'une harmonisation intégrée dans un cadre le plus global[38]. La promotion de la coopération internationale, la réalisation de lignes directrices au sujet des problématiques de protection des données et les « règles entre Etats » contribueraient à résoudre les difficultés actuellement rencontrées[39]. Les définitions des concepts devraient ainsi être clarifiées, tout comme leur application dans les Etats membres[40].

175. Plusieurs répondants soulignent le caractère potentiellement universel – ou mondial – de la Convention du Conseil de l'Europe et l'intérêt de la promouvoir sur le plan international, comme **standard global**[41]. D'ailleurs, la résolution de Madrid, universellement acceptée, pourrait inspirer la rédaction de certains principes de la Convention 108[42]. Ces considérations valent tant quant aux questions d'applicabilité des droits nationaux, que quant aux flux transfrontières de données ; les problématiques sont clairement liées.

176. **Règle déterminant le droit applicable à la protection des données**. La complexité de la question du droit applicable est évoquée dans certains des avis communiqués, notamment dans des contextes tels que celui du « Cloud Computing »[43]. Ainsi, certaines parties soulignent qu'il serait compliqué de trancher cette question au sein de la Convention, notamment eu égard au rôle joué par

[35] Avis Data Industry Platform ; avis FEDMA.

[36] Avis CNIL.

[37] Voy. par exemple avis Techamerica Europe.

[38] GS1 in Europe.

[39] Avis CEA.

[40] Avis EFAMRO-ESOMAR.

[41] Avis de l'AEDH ; avis de l'AFAPDP et l'OIF ; avis CNIL ; avis Spyros Tsovilis ; avis Direcção-General da Politica de Justica .

[42] Avis CNIL.

[43] Voy. par exemple avis UK Ministry of Justice .

l'Union européenne en la matière[44] ; il faut se coordonner. Clairement, les réflexions doivent être poursuivies en la matière, mais peut-être que la complexité du problème nécessiterait de traiter les hypothèses au cas par cas plutôt que d'établir une règle générale sur la question.

177. Il n'empêche, de nombreux répondants pensent que la question devrait être traitée dans la Convention[45] – de manière coordonnée avec la directive 95/4646 –, ou qu'il serait en tout cas souhaitable qu'il en soit ainsi[47] [48]; c'est préférable pour la sécurité juridique. D'autres relèvent que l'intégration d'une telle disposition pourrait, le cas échéant, constituer un obstacle pour une éventuelle ratification de la Convention 108 par des Etats tiers au Conseil de l'Europe[49], alors qu'il conviendrait d'en faire un instrument attractif pour ces Etats[50]. Or la protection des données et la vie privée sont des problématiques très complexes et techniques au sein desquelles demeurent des débats politiques non résolus[51]. Des sondés notent que la Convention devrait consacrer un principe général, le surplus relevant des réglementations nationales et de la coopération internationale[52]. Mais un sondé considère qu'il n'est simplement pas désirable que la Convention tranche la question du droit applicable à la protection des données[53].

178. Quoi qu'il en soit, différents avis offrent des pistes de réflexion quant à la détermination du droit applicable à la protection des données.

179. Au niveau des **critères de rattachement**, différentes propositions se dégagent des avis. Par exemple, chaque Etat garantissant une protection équivalente – on se situerait, par exemple, au sein de l'Union européenne –, une entreprise agissant dans plusieurs de ces Etats ne serait tenue au respect que d'une seule réglementation : celle de son lieu de principal établissement[54]. Selon certains répondants, les règles de chaque Etat devraient être considérées équivalentes[55]. On

[44] Avis commun de l'AFME et de la BBA.

[45] Avis Bulgaria-Commission pour la protection des données personnelles ; Avis Cyprus-Data Protection Commissioner; Avis Czech Republic – The office for personal data protection; avis Lithuania-State data protection inspectorate ; avis Ile Maurice-Commissariat à la protection des données; avis mydex (point 24) ; avis Ukraine-Data protection authority.

[46] Avis EPA; Avis German Insurance Association.

[47] Avis CNIL ; avis Cyberspace Law and Policy Centre ; avis EBF ; avis CLSR-IAITL-ILAWS ; avis Privacy International. Le T-PD devrait ainsi étudier la question, avis Direcção-General da Politica de Justica .

[48] Dans l'avis Albania-Data Protection Commissioner, il est souligné qu'il faudrait prévoir dans la Convention une règle permettant aux Etats d'établir des règles spécifiques en la matière.

[49] Avis CNIL.

[50] Avis CLSR-IAITL-ILAWS.

[51] U.S. Federal Trade Commission.

[52] Ukraine-Ministry of justice.

[53] Avis Italy-Garante per la protezione dei dati personali.

[54] Avis EPA.

[55] Avis APEP.

observe de manière générale que certains répondants souhaitent le jeu d'un « country of origin principle »[56].

180. D'autres nuances sont proposées quant aux critères de rattachement. Certains proposent que soit pris en compte, à titre principal, le critère du lieu d'établissement du responsable de traitement et qu'à titre secondaire, ce soit celui du lieu vers lequel le responsable de traitement dirige son activité de façon spécifique[57]. Le critère de la direction des activités serait un critère à prendre en compte en particulier lorsque le responsable de traitement est établi en dehors du territoire de l'UE[58]. Il est parfois suggéré que le droit du pays où la plus importante part des opérations de traitement a lieu soit applicable ou, si cela ne peut être déterminé, le droit du pays de localisation du responsable de traitement[59].

181. Dans un autre sens, des répondants vont jusqu'à considérer que lorsque plusieurs juridictions sont concernées, « les personnes concernées devraient être en droit de se réclamer de la législation la plus protectrice en cas de problème »[60]. Ou encore, que le droit applicable à la protection des données devrait être celui de la « victime »[61] – personne concernée. Le cas échéant, cette règle vaudrait en tant que principe et des exceptions pourraient être aménagées[62].

182. Quels que soit les critères finalement retenus, des **considérations à prendre en compte** dans leur définition sont évoquées par les sondés. Ainsi, s'il s'agit de veiller à réduire le risque de « *forum shopping* »[63], il faudrait aussi limiter les « *compliance burdens* » pesant sur les entreprises[64]. Dans le même sens, une simplification des règles est demandée quant aux entreprises appartenant à un même groupe international ayant des activités transfrontières[65], notamment en clarifiant les responsabilités au sein de tels groupes.

183. Certains jugent que toute évolution des règles en cause devrait impliquer une amélioration de la libre circulation des données à caractère personnel[66]. La modification des règles de droit international privé ne doit pas entraîner un désavantage compétitif pour le marché intérieur (UE)[67]. Il ne faudrait pas non plus

[56] Avis FEDMA ; avis Techamerica Europe .

[57] Avis CNIL

[58] Avis APEP

[59] Avis EPA

[60] Avis de l'AEDH

[61] Avis Sénégal-Commission à la protection des données.

[62] L'avis Direcção-General da Politica de Justica semblerait aller dans le même sens, recommandant l'applicabilité de la loi de la personne concernée, en ce qu'il renvoie à la « loi nationale ». Il souligne toutefois que des exceptions devront certainement être adoptées, en particulier quant au contexte de l'Union européenne.

[63] Avis CEA.

[64] Avis CEA ; avis EMOTA ; avis ENPA-FAEP; FEDMA.

[65] Avis Data Industry Platform ; avis GDD.

[66] Avis commun de l'AFME et de la BBA ; avis Data Industry Platform ; avis EMOTA ; avis FEDMA.

[67] Avis APEP.

introduire une « *extra jurisdictional reach* »[68]. Pour éviter ce dernier travers, il serait recommandé de tenir compte de la volonté des individus de recourir aux services de prestataires totalement en dehors de l'Espace Economique Européen (EEE-EEA), et privilégier la prise de décision correctement informée[69].

184. Dans un autre ordre d'idées, les règles déterminant le droit applicable ne devraient pas permettre, aux demandeurs en justice contre des entreprises de médias, de choisir un forum où les règles de protection sont plus strictes que celles de l'Etat d'établissement de ces entreprises, ce qui entraînerait un risque pour la liberté d'expression[70].

185. Une disposition de la Convention sur le droit applicable ne devrait pas contrarier la protection nationale offerte aux consommateurs[71].

186. Il faudrait encore prendre en compte le fait que la modification des règles déterminant le droit applicable n'ont pas seulement une incidence sur les relations « B2C » mais également sur les relations entre entreprises et autorités gouvernementales, dont les « *law enforcement authorities* »[72].

187. Enfin, si la question du droit applicable est souvent traitée par les avis rendus, certains évoquent les critères de compétence et la nécessité qu'ils soient pragmatiques – le cas échéant, une distinction pourrait aussi être opérée entre la compétence civile et la compétence pénale ; il conviendra que le T-PD se penche sur cette question[73].

Autorités de protection des données

25. Comment garantir leur indépendance et assurer une coopération internationale entre les autorités nationales ?

188. Une meilleure coopération est demandée[74]. Des répondants relèvent que la coopération entre autorités de protection des données devrait sans doute faire l'objet de mesures complémentaires inscrites dans la Convention[75] – d'autres ne sont pas du même avis, laissant le problème au droit national[76] –, de mécanismes internationaux facilitant la coopération transfrontière pour l'application des droits de la protection des données[77], mécanismes à définir – tels qu'un forum commun[78] ; le

[68] Avis commun de l'AFME et de la BBA.
[69] Avis commun de l'AFME et de la BBA.
[70] Avis ENPA-FAEP.

[71] Avis CIPPIC.

[72] Avis Techamerica Europe .

[73] Avis Direcção-General da Politica de Justica.

[74] Avis commun de l'AFME et de la BBA.
[75] Avis AEDH

[76] Avis CLSR-IAITL-ILAWS ; avis Privacy International ; avis Ukraine-Ministry of justice.

[77] Avis EBF.

minimum d'exigences devrait en tout cas être prévu[79]. Il s'agirait alors de préciser et faciliter la coopération internationale – conditions de coopération, modalités des actions communes –, mais de ne pas l'imposer[80]. Certains estiment au contraire que la coopération doit être imposée pour les problèmes globaux[81].

189. Il est aussi proposé que les autorités puissent conduire des investigations conjointes sur le territoire de plusieurs Etats membres – plaintes internationales, contrôles transfrontières – [82], sans pour autant que cela ne mette en péril leur financement[83]. Dans ce cadre, il importe de clarifier les pouvoirs d'actions des autorités à l'étranger[84]. D'autres notent qu'il devrait être travaillé à une meilleure reconnaissance entre autorités de protection des données des mesures prises par elles – y compris les notifications[85]. Un répondant va jusqu'à proposer la création d'une autorité supranationale[86].

190. Il a enfin été relevé que l'article 13, § 3, b), de la Convention était un obstacle à la coopération internationale entre autorités en ce qu'il empêchait le transfert des données à caractère personnel impliquées dans le traitement litigieux alors que cela est nécessaire en vue de la résolution des différends[87].

191. Concernant l'indépendance de ces autorités de contrôle, la Direcçao Geral da Politica de Justiça portugaise propose les critères suivants : Il faut des garanties que l'autorité de protection des données n'est pas assujettie à des instructions ou à des conditions susceptibles de gêner sa capacité de décision indépendante, c'est-à-dire sans une quelconque interférence d'aucune entité publique ou privée, et qu'elle dispose, par le biais du budget public, des moyens nécessaires à son fonctionnement.

26. Leur rôle et leurs tâches devraient-ils être spécifiés ?

192. Oui. L'AEDH relève que le protocole additionnel est peu explicite sur les missions et les pouvoirs des autorités de contrôle. Les exemples contenus dans le rapport explicatif mériteraient tous d'être codifiés dans le texte même du protocole. Le CLPC invite à transférer la disposition dans la Convention elle-même.

---

[78] Avis Italy-Garante per la protezione dei dati personali.

[79] Avis Lithuania-State data protection inspectorate.

[80] Avis CNIL.

[81] Avis APEP.

[82] Avis Bulgaria-Commission pour la protection des données personnelles ; Avis CNIL.

[83] Avis Bulgaria-Commission pour la protection des données personnelles.

[84] Avis CNIL.

[85] Avis Techamerica Europe.

[86] Avis Sénégal-Commission à la protection des données.

[87] Avis United Kingdom-Information commissioner's office.

193. Pour le ICUK, une clarification serait la bienvenue dans un paysage où les autorités nationales existantes présentent un patchwork bigarré. Leur rôle éducatif devrait en tout les cas être maintenu. La CNIL estime qu'il conviendrait de renforcer le pouvoir de contrôle *a posteriori* de ces autorités. La Commission bulgare demande qu'on veille à ne pas surcharger de manière infondée ces autorités. Le CLPC insiste sur une tâche en particulier : l'obligation de rendre des comptes notamment au public sur les obligations de traiter les plaintes. Tandis que pour le Garante il serait important d'apporter des précisions sur les mécanismes de coopération entre autorités, peut-être en envisageant des mécanismes d'interaction spécifiques ou des forums communs.

194. En outre, aux yeux de l'EPA et de l'APEP, leurs décisions devraient être reconnues mutuellement par les autres Etats Parties, ce serait appréciable, notamment concernant les BCR. Le CIPPIC invite à réfléchir à rendre les décisions des autorités de contrôle juridiquement liantes par le biais du concept de *common law* de *stare decisis*.

Flux transfrontières de données

27. La Convention 108 avait pour but de concilier la protection effective des données et la libre circulation de l'information sans considération de frontières. Ces principes ont été développés plus avant dans un protocole additionnel (STCE 181, 2001). En principe, un niveau de protection adéquat doit être assuré.

28. Doit-on entièrement réexaminer la notion de « flux transfrontières de données » à l'heure d'Internet, où les données circulent instantanément à travers les frontières ? Serait-il utile de fixer des règles minimales internationalement reconnues pour garantir le respect de la vie privée sans considération des frontières ? Quel pourrait en être le contenu ?

29. Doit-il y avoir des règles différentes pour le secteur public et le secteur privé ? S'agissant notamment du secteur privé, doit-on avoir davantage recours à des règles d'entreprise contraignantes, éventuellement associées à un système de responsabilisation du destinataire final pour garantir le respect de ces règles ?

195. Les questions relatives aux FTD sont à lire en parallèle avec la problématique du droit applicable à la protection des données. Un répondant émet un avertissement : dans un monde en réseau, il y a des limites à la mesure dans laquelle les flux de données peuvent ou doivent être contrôlés[88].

196. Différents intervenants soulignent que l'approche actuelle du régime des flux transfrontières de données n'est pas adaptée à la situation actuelle du contexte technologique[89] ; les individus impliqués dans le monde virtuel font passer leurs données d'une juridiction à l'autre via de simples clicks, le cas échéant à destination

[88] Avis CLSR-IAITL-ILAWS.

[89] Avis commun de l'AFME et de la BBA ; Avis Czech Republic – The office for personal data protection .

de pays tiers à l'UE ne garantissant pas de protection adéquate[90]. L'approche actuelle ne fonctionne pas de manière efficace, étant pesante pour ceux agissant de manière bénigne, et inefficace vis-à-vis de ceux qui sont plus malicieux[91]. La problématique des FTD devrait être traitée de manière plus réaliste[92]. A tout le moins, il devrait être spécifié, dans le contexte d'Internet, quand ont lieu de tels transferts[93] ; le concept de FTD doit être clarifié voire reconsidéré[94]. A l'occasion de la revendication d'un système plus praticable, les travaux de l'APEC ont été évoqués[95].

197. Différents répondants estiment que « l'approche de principe » « ne devrait pas être modifiée » en ce qu'une protection adéquate est exigée[96]. Dans le même sens de l'exigence d'une protection adéquate, il a été souligné que les dispositions du protocole additionnel devraient être intégrées à la Convention[97], le cas échéant en précisant les règles[98]. Au contraire, certains demandent un nouvel instrument légal, séparé de la Convention, et contenant les règles détaillées nécessaires[99]. D'autres encore notent que le caractère de la Convention est général et qu'il appartiendrait plutôt aux Etats membres de traiter cette question compliquée[100], alors que les différences nationales exacerbent les difficultés pratiques actuelles[101].

198. La définition de l'adéquation intéresse les répondants. Des répondants considèrent qu'il faudrait établir une liste des garanties minimales définissant le standard du niveau adéquat de protection[102], le cas échéant en s'inspirant de ce qui se fait au niveau de l'Union européenne[103]. Selon certains, la Convention 108 devrait expressément reconnaître les décisions d'adéquation de la Commission européenne prises sur le pied de l'article 26 de la directive 95/46[104]. D'autres critiquent toutefois ce qui se fait au niveau européen en soulignant que ce qu'exige la Commission

[90] Avis Techamerica Europe .

[91] Avis CLSR-IAITL-ILAWS.

[92] Avis United Kingdom-Information commissioner's office.

[93] Avis Albania-Data Protection Commissioner ; avis Bulgaria-Commission pour la protection des données personnelles.
[94] Avis EBF ; Avis Italy-Garante per la protezione dei dati personali.

[95] Avis U.S. Federal Trade Commission.
[96] Avis de l'AEDH. Favorable à l'exigence du standard de la protection adéquate, voy. encore avis UK Ministry of Justice.
[97] Avis Cyberspace Law and Policy Centre ; avis CLSR-IAITL-ILAWS ; avis Privacy International ; avis Direcção-General da Politica de Justica.

[98] Avis CLSR-IAITL-ILAWS.

[99] Avis Cyprus-Data Protection Commissioner.

[100] Avis FEDMA.

[101] Avis CLSR-IAITL-ILAWS.

[102] Avis Albania-Data Protection Commissioner ; avis Bulgaria-Commission pour la protection des données personnelles.
[103] Avis Albania-Data Protection Commissioner .
[104] Avis APEP.

relève parfois plus de l'équivalence que de l'adéquation[105] ; la Convention devrait réaffirmer que ce n'est que l'adéquation qui est exigée[106]. Aussi, le processus pourrait être plus rapide et plus simple[107]. La Convention pourrait rendre le processus d'évaluation plus transparent et pourrait dans ce cadre être à la source du développement de standards largement reconnus[108].

199. Plus spécifiquement, il est suggéré que l'appréciation du caractère adéquat puisse être effectuée sur la base de larges secteurs de traitement de données – secteur financier, sous-traitance informatique, PNR, etc. – [109] ; par ex., un secteur serait réputé garantir une protection adéquate, même si le pays de son établissement n'offre pas des garanties adéquates de protection[110]. Ainsi, l'adéquation ne devrait pas être une analyse générale du droit de l'Etat tiers concerné, mais elle devrait être plus liée aux circonstances particulières du cas d'espèce, en particulier au responsable de traitement – ou sous-traitant – situé dans l'Etat tiers, le droit de cet Etat n'étant qu'un élément d'analyse parmi d'autres[111]. Certains lient aussi directement le principe de la protection adéquate au principe d' « *accountability* »[112].

200. Dans le contexte de l'Union européenne, lorsqu'un pays tiers ne garantit pas une protection adéquate, différents outils peuvent néanmoins permettre les FTD. A cet égard, certains demandent qu'il y ait, dans le contexte de l'Union européenne, une meilleure reconnaissance des « *Binding Corporate Rules* » [BCR] ou « *Model Contractual Clauses* » [MCC], de telle sorte que les transferts de données ayant lieu au sein d'un même groupe international d'entreprises soumis aux mêmes règles strictes ne doivent pas faire l'objet d'une autorisation spécifique des autorités de protection des données[113] ; les règles devraient être simplifiées[114]. Le régime d'autorisation est problématique quant au temps et aux frais qu'il nécessite[115], il conviendrait de procéder à un allègement des formalités en cas de recours aux MCC ou aux BCR approuvées par les autorités[116]. Plus de flexibilité est d'ailleurs demandée quant aux clauses contractuelles types qui, à l'heure actuelle dans l'Union européenne, ne reflètent par exemple pas la réalité du « *Cloud Computing* », rendant le modèle inapproprié[117]. Il serait également opportun de promouvoir des

[105] Avis CLSR-IAITL-ILAWS.

[106] Avis United Kingdom-Information commissioner's office.

[107] Avis United Kingdom-Information commissioner's office.

[108] Avis CLSR-IAITL-ILAWS.

[109] Avis Albania-Data Protection Commissioner; avis APEP.

[110] Avis United Kingdom-Information commissioner's office.

[111] Avis United Kingdom-Information commissioner's office. Constate également que la situation du receveur des données n'est pas prise en compte l'avis U.S. Federal Trade Commission ; avis UK Ministry of Justice, faisant référence à la Déclaration de Madrid comme point de départ de la réflexion.

[112] Avis Techamerica Europe ; avis United Kingdom-Information commissioner's office.

[113] Avis commun de l'AFME et de la BBA.

[114] Avis Data Industry Platform; avis EMOTA.

[115] Avis German Insurance Association.

[116] Avis AFCDP (p. 4).

[117] Avis commun de l'AFME et de la BBA.

codes de conduite sur les FTD qui seraient acceptés par toutes les autorités de protection des données pertinentes[118].

201. Des répondants considèrent que des règles internationales minimales devraient être établies quant aux FTD[119]. Ce qui est l'objectif de la résolution de Madrid qu'il conviendrait d'incorporer dans un texte liant[120]. Mais dans toutes les hypothèses où de telles règles minimales seraient souhaitables, il conviendra de garder en vue le potentiel risque d'une « *race to the bottom* »[121] ; des répondants estiment qu'une telle course serait la conséquence nécessaire d'une tentative d'établir des règles minimales globales, détruisant la protection de la vie privée dans un contexte transfrontière, et rendant donc ce minimum non souhaitable[122]. D'autres rappellent qu'avant de penser aux standards minimums globaux, il faudrait établir le cadre procédural de leur élaboration, mettant en jeu toutes les régions et tous les intéressés[123].

202. Enfin, dans un autre registre, le « *Data Protection Officer* » [DPO] pourrait avoir un rôle en matière de FTD, et un DPO européen pourrait être nommé pour un groupe de sociétés présent dans différents pays de l'Union européenne[124].

[118] Avis CEA.

[119] Avis CEA ; Avis Cyprus-Data Protection Commissioner; Avis EPA ; Avis German Insurance Association; avis AFCDP.

[120] Avis APEP.

[121] Avis CIPPIC.

[122] Avis Cyberspace Law and Policy Centre; avis CLSR-IAITL-ILAWS ; avis Privacy International .

[123] Avis U.S. Federal Trade Commission.

[124] Avis AFCDP.

Rôle du comité consultatif

30. La Convention 108 a créé un comité chargé de faciliter son application et, le cas échéant, de l'améliorer. Doit-on renforcer le rôle jusqu'ici principalement consultatif du comité ? Si oui, quelles fonctions faut-il développer plus avant : l'activité normative, le règlement des litiges, le suivi ?

203. La plupart de ceux qui ont répondu à cette question sont favorables au renforcement du rôle du Comité consultatif, tandis que quelques répondants estiment que le rôle doit demeurer inchangé.

204. Le Comité devrait évoluer vers une véritable autorité de protection des données, chargée en matière de suivi d'identifier très en amont les innovations et de les accompagner de recommandations, et en matière de litige, de pouvoir être saisie lorsque des parties prenantes sont confrontées à un problème transfrontalier (AEDH). Le Commissaire à la protection des données de l'Ile Maurice souligne qu'en matière de litiges, il conviendrait que les autorités nationales mais aussi les individus puissent saisir ce Comité transformé en autorité contraignante. Un rôle de suivi renforcé permettrait de vérifier la manière dont la Convention est mise en œuvre au niveau national et de disposer de moyens d'action en cas de mauvaise mise en œuvre (CNIL). Un renforcement du rôle ne devrait porter que sur des fonctions de surveillance (CEA Insurers of Europe), ou sur ces fonctions mais également sur l'édiction de standards (Commissaire à la protection des données de Chypre ; consortium CLSR-IAITL-ILAWS), voire que sur l'édiction de standards (European Privacy Association). Un rôle de coordination des pratiques, expériences et suggestions des autorités nationales de protection des données devrait être assumé par ce Comité, de même qu'un rôle de suivi au niveau de la coopération internationale (Office for National Data Protection de la République tchèque ; State Data Protection Inspectorate de Lituanie). Enfin, on devrait leur reconnaître un rôle d'élaboration législative.

205. Il faut toutefois veiller à ce que cela n'induise pas des charges supplémentaires pour les Etats parties et pour les autorités nationales. Il faudra être attentif à éviter toute duplication avec les autres organismes supranationaux existants et éviter d'adopter des standards contradictoires (ICUK). Pour la Data Industry Platform, le risque de duplication est avéré et ils sont opposés à l'idée d'ajouter une couche supplémentaire aux institutions déjà existantes. Pour eux, l'élaboration de standards, la résolution de litiges et les fonctions de suivi sont des matières dans lesquelles l'autorégulation est la réponse la plus adéquate.

206. L'autorité de protection des données chypriote et le Garante italien relèvent tous deux que tout renforcement de rôle du Comité sera dépendant d'une mise à disposition de moyens humains et financiers. Pour le Garante, il conviendrait donc d'adopter des dispositions visant à garantir la mise à disposition de telles ressources.

207. La CNIL fait une suggestion à propos de la composition de ce Comité. Etant donné le rôle « absolument essentiel » de ce comité dans l'architecture du travail du Conseil de l'Europe, la CNIL estime qu'il serait extrêmement souhaitable de revoir la composition de cet organe. Etant donné que ce sont les autorités de protection des données qui sont les premières en charge d'appliquer la Convention 108, que ces autorités bénéficient de l'expérience et de l'expertise pratique, à l'inverse du gouvernement, ce devrait être elles qui désignent un représentant pour composer le

Comité et non les gouvernements. Les représentants de gouvernements sont eux les seuls présents au Comité directeur de coopération juridique qui intervient dans le processus d'élaboration des textes.

208. La FTC américaine suggère que la révision de la Convention soit l'occasion de réfléchir à l'apport et au soutien que le Comité pourrait rechercher auprès de l'industrie et d'autres acteurs clés. Le rôle et le travail de l'ENISA Permanent Stakeholder Group pourrait peut-être être pris comme exemple de comment obtenir un apport et faciliter le dialogue avec l'industrie sur la Convention, étant donné le rôle important que ce groupe joue dans le cadre juridique de la protection des données de l'UE et ailleurs dans le monde.

INTRODUCTION

1. The public consultation organised by the Council of Europe in order to ascertain the reactions of all parties concerned to the idea of modernising Convention 108 met with great success. The Secretariat of the Council of Europe received numerous contributions, most of which were detailed and backed up by arguments and analyses based on the expertise or practical experience of the contributors. Moreover, some of the latter joined forces and presented a joint response to the questionnaire, while certain federations or groups expressed their opinion on behalf of all their members.

2. Every kind of background was represented in the replies – the public sector (governmental authorities, data protection authorities etc.), the private sector (the worlds of banking, insurance, electronic commerce, marketing, audiovisual distribution, socio-economic research etc.), and the academic world and interested associations.

3. There was also a geographic spread. Replies came from various parts of Europe, and not only from European Union countries but also from states outside it such as Albania and Ukraine. It is interesting to compare the replies from states covered by the European data protection directive (European Union area) with those from north America (United States and Canada), Africa (Senegal, Mauritius) and Australia. The International Organisation of La Francophonie also sent comments.

GENERAL CONSIDERATIONS

4. The replies received sometimes suggest a direction to be followed but do not indicate the means of giving practical effect to that approach. Sometimes, by contrast, commentators present arguments and pointers to one or other direction.

5. In a number of cases, contributors state that in view of the difficulty of the matter, an in-depth study ought to be carried out. This was said, for example, about the exclusion from the scope of the Convention of data processing for personal and household purposes or on the question of the law applicable. In other cases, contributors call for an impact analysis or a study of the effectiveness of the legislative measures envisaged (in particular concerning the introduction of the possibility of class actions and systems of alternative dispute resolution, or concerning the introduction of a duty to report data breaches).

6. Many contributors argue that the work of modernising the Convention should be carried out from a concern to achieve the greatest possible consistency with the protection rules laid

down by the European Union (mainly Directive 95/46). Thus in many cases replies were guided by this concern to align the text of the Convention with that of the European directive. The work of modernising that directive, currently in progress, should be monitored so as to ensure that discrepancies between the texts do not arise. It is interesting to note that this concern is voiced not only by persons from the European Union: it is shared by people outside the EU.

OBJECT AND SCOPE OF THE CONVENTION, DEFINITIONS

1. Convention 108 has been drafted in a "technologically neutral" approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

7. All those who replied were in favour of keeping the text simple and setting out general principles.

8. In their opinion, this is the only approach which guarantees the long-term viability of the Convention. The past thirty years, with a convention laying down general principles, have shown that this model has stood the test of time.

9. In the same long-term perspective, everyone likewise emphasises the need to ensure the technologically neutral nature of the Convention. The principles formulated must not focus on the existence of a technology, for that would incur the twofold risk that the principles might become obsolete once the technology is outdated or abandoned, and that the principles would not be adaptable to the new technologies that will inevitablyemerge.

10. That being said, the replies state that, while the text of the Convention should not be made too detailed, it is nonetheless necessary to make some additions to the existing text.

11. Several contributors draw attention to the fact that, if the Convention is to have universal validity in the future, it must be realised that too detailed a text will undoubtedly scare away states which might be considering accession to the Convention.

12. Consequently, some commentators take the view that the existing approach should be pursued – keeping the text of the Convention general and simple, and setting out the general principles in detail in specific texts (Committee of Ministers recommendations).

2. Should Convention 108 give a definition of the right to data protection and privacy?

13. Some of those who replied to this question believe that including definitions of the right to data protection and the right to respect for privacy would help to clarify the scope of the text and help the public to understand its subject-matter. In the view of APEP (the Spanish Professional Association for Privacy), this would make it clear that private life and data protection are two different rights, and that personal data may or may not be private.

14. Others consider that, as the concept of privacy appears in several international legal instruments, it would not be opportune to define it in Convention 108. In particular, it is the responsibility of the European Court of Human Rights to define the scope of this concept as set down in Article 8 of the European Convention on Human Rights. The CNIL, for example, considers that these concepts should not be defined but left open to interpretation in an evolutive way. The State Data Protection Inspectorate of Lithuania points out that the international legal instruments which protect private life do not give any definition of it. The same approach could be adopted with regard to data protection.

15. Let us note in passing that a non-uniform perception of what privacy means is discernible in the replies. Some of them refer to the conventional meaning (intimacy, confidentiality), not the more developed one of autonomy and information control as updated by the European Court of Human Rights. The European Banking Association, which believes that Convention 108 should contain the definitions in question, also states that this is particularly important in so far as the Convention is to serve as a basis for countries outside the European Economic

Area, which do not have specific definitions in their own legislation or any knowledge of the concepts of “privacy” and “data protection” in case-law and doctrine in relation to existing European definitions.

16. On the other hand, with regard to the concept of the right to data protection, these and other contributors appreciate the value of a definition while calling for its harmonisation with the one given in the Charter of Fundamental Rights of the European Union. Privacy International emphasises in this connection that it is worthwhile trying to define the right to data protection, in view of the fact that many of the world’s constitutions have begun to recognise that data protection is indeed a right.

17. Some replies argue that defining concepts after 30 years’ application of the text is not justified. That length of time brings an opposite response from Portugal’s Direcçao Geral da Politica de Justiça, which considers that, as the oldest instrument of public international law on the matter, Convention 108, which claims to regulate data protection law, must not demonstrate an inability to define that right itself.

18. The European Newspaper Publishers Association does not state its opinion on the desirability of including such definitions, but says that, if the decision is taken in favour of definition, care should be taken not to make the inference that these rights would prevail over those of freedom of expression and information. Introducing legal uncertainty must also be avoided.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement agencies. Should this comprehensive approach be retained?

19. There is unanimous agreement that an approach which covers both the private sector and the whole of the public sector, including police and justice system, must be maintained. Given the practical ease and potential of existing technical tools (not to mention those that will emerge in future), it is considered “absolutely vital”, to quote many contributors, that law enforcement personnel be required to respect data protection principles.

20. Of course, everyone agrees on the need to adapt these principles to allow for needs arising from the work of these players. The important thing is not to leave the police and justice system outside the protection sphere. The solution generally envisaged is a series of partial exceptions for these players.

21. TechAmerica Europe proposes that thought be given to situations in which partly different rules would apply to public authorities and private entities, while keeping the same basic principles and requirements as to transparency. They ask for consideration to be given to the impact which changes to the Convention might have on the work of law enforcement in order to check that these new measures or new concepts do not give rise to particular difficulties in this sector.

22. Another American contributor asks for special care to ensure that any change made to the Convention continues to allow of a degree of flexibility in exchanges of “police” data between the United States and Europe and permits data sharing for purposes of public safety and prosecution of offences.

23. The Canadian contributors emphasise that their experience of two separate sets of rules for the public and private sectors, as at federal level in Canada, has given rise to criticisms from civil society and from the Federal Privacy Commissioner.

4. Convention 108 does not exclude from its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

24. Generally speaking, those who replied are in favour of introducing an exception to the scope of the Convention for data processed for personal or household purposes.

25. Many of them stress that this must be done in a concern to align the Convention's protection model with that of Directive 95/46.

26. However, several contributors think it will be extremely difficult to decide exactly what such an exception would cover.

27. The AEDH, which is in favour of this exception, proposes making it conditional on data not being communicated to third parties and that the exception goes hand in hand with an obligation on services supporting such personal activities (electronic mail, address book, diary, archive service etc.) to inform their clients about their obligations and offer them confidentiality functions.

28. The CNIL suggests following the European Union model and stating that it lies within the power of interpretation of the national supervisory authorities to define what comes under the exception and what does not.

29. The CIPPIC (Canada) observes that this question was mentioned as being a future challenge in the data protection field. At all events, there must be careful balancing with the right to freedom of expression when it comes to settling this question of individuals' private activities. It was precisely when giving consideration to freedom of expression as against data protection that the Centre for Socio-Legal Studies developed its standpoint on this exception hypothesis. Realising that many of the situations in which personal data are processed in the most intrusive and unwarranted way are the result of private individuals motivated by non-commercial reasons, the Centre does not wish these activities to be excluded from the scope of all protection rules. In its opinion, a better solution would be, first to ensure that such individual activities can benefit fully from a new and broader clause on freedom of expression, and then to impose on individuals just some of the obligations of file controllers, determined in a clear, proportionate manner.

30. The European Privacy Association, whose views on this point are shared by the APEP (the Spanish Professional Association for Privacy) and by the State Data Protection Inspectorate of Lithuania, points out that the activities of individuals nowadays may easily harm others and therefore their activities cannot be wholly excluded from data protection rules. On the other hand, however, purely personal activities cannot be made subject to disproportionate obligations and burdens, especially in relation to security (Article 7) and transborder flows (Article 12). The APEP stresses that regulations must be able to sanction the misuse of personal data by individuals. This association would consider it disproportionate to place obligations on individuals such as having to declare data processing, to provide information in accordance with Articles 10 and 11 of Directive 95/46, to take security measures or to ensure that such measures are being taken by the platform they are using.

31. Senegal's Data Protection Commission suggests that, over and beyond the proposed exception, which it supports, it be broadened by the addition of "processing of data not intended for systematic communication to third parties or for distribution".

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

32. All who replied favour including the concept of collection in that of automatic processing. This stance is motivated primarily by the desire to ensure consistency with European, national and international standards. There is also the belief that it is useful for collection to be made subject to all the principles governing data processing, not just to one particular provision.

33. The concern for consistency among legal systems also explains why many contributors, such as CEA Insurers of Europe or the AFME BBA (banking & financial services), call for the adoption of the concept of "processing" as presented in the European directive. The CEA considers that it would be helpful for the "disclosure by transmission" operation, which is a fundamental operation in data processing, to be expressly included in the list of operations covered. The CNIL believes that the concept of processing should be as broad as possible, so great is the tendency for operations carried out on data to grow in number and diversity.

34. The AFME BBA, like the European Banking Federation, points out that the terminology must not be confined to such concepts as "file" which have a dated technological connotation that could compromise both the neutrality of the text and the broad application of the Convention, as this notion is no longer relevant in the present-day Internet and cloud computing situation.

35. Lastly, the Portuguese Direcçao Geral da Politica de Justiça asks us to reflect on the broadening of the scope of the Convention to include non-automatic processing. That body is aware that such processing is a minority today, but considers that it has not entirely disappeared and that prudence requires its inclusion in the sphere of protection.

The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?

36. Some contributors think that the current version of the Convention should not be amended on this point. The present definitions are sufficient to render the persons involved in data protection responsible.

37. Others believe that the definition of "responsable du traitement/data controller" used in Directive 95/46 should be substituted for that of "controller of the file".

38. The Data Protection Commissioner of Mauritius proposes replacing the definition by the following one: "The controller of the file is any natural or legal person, whether public or private, who decides on any activity, whether automated or not, carried out on personal data". The APEP - Spanish Professional Association for Privacy proposes that the definition be amended to include "any person or persons who has/have the de facto right to decide on the purpose and means of processing personal data, either by virtue of the law or in accordance with a contractual agreement with the person concerned or a third party". That body considers it important, for reasons of legal certainty, that only persons having legal personality should be responsible for processing.

39. Several replies observe that it would be desirable to allow for cases in which there are several persons responsible for processing the same data. The AEDH quotes the example

of a decision to use a file taken by a number of responsible persons for joint purposes, such as compiling a file common to a trade or profession in relation to defaulting customers. The APEP draws a distinction between joint controllers (processing the same data for the same purpose) and several controllers (processing the same data but for different purposes).

40. The European Privacy Association draws attention to the fact that advanced technologies (such as cloud) are increasingly resulting in the automated processing of data by multiple agencies. This association believes it is important, not to state the names and functions of those agencies but to define the processing activities, the requirements and obligations linked to those activities and the related responsibilities. This view is shared by the Information Commissioner for the United Kingdom (ICUK), who says that, rather than listing the criteria for what constitutes a "controller", he would prefer there to be a better description of the activities which a file controller may carry out.

41. EFAMRO ESOMAR (research sector) thinks it necessary to introduce a clearer definition of "data controller", laying responsibility on the shoulders of the persons who decide how data are to be processed, as distinct from those who control a particular computer system or file. This would make just one data of the file responsible for assessing the need to process data and the security of the available systems before opting to process data using such systems. It would also provide citizens with a single focus of responsibility and accountability.

42. The German Insurance Association would welcome a review of the concept of file controller, because it would present an opportunity to make changes in data processing in the world of business. Centralisation of service tasks within groups and recourse to outsourcing of tasks to competent services are the principal areas concerned. Being able to present the entity transferring data and the one receiving them jointly as a single entity responsible for processing would facilitate data transfer and simplify group life.

43. That standpoint echoes a remark made by the Computer Law and Security Review consortium, the International Association of IT Lawyers and the Institute for Law and the Web (University of Southampton): they point out that in a network environment, the concept of controller of the file is no longer as relevant as before, because of the increasing use of systems of data sharing and interconnection. In such environments, it would be preferable to appoint a single entity to take overall responsibility (as in the European Union systems of binding corporate rules). An obligation should be placed on those responsible for individual processing to inform the persons concerned of any data sharing and interconnection involving them and provide particulars of the coordinating entity.

44. Lastly, Mydex Community Interest Company states – and says that its view is shared by many others, including the World Economic Forum – that in future, the technical architectures of future generations will place individuals at the centre of their own personal data ecosystems, so that they will themselves take responsibility for processing. The legislation will have to reflect this new modus operandi and permit this "data empowerment by design".

6. New definitions may be necessary, such as for the sub-contractor or the manufacturer of technical equipment.

45. Contributors welcome the intention to introduce new definitions if it is done in a concern for consistency with those developed in the European Union. That would make it possible to improve legal certainty, enhance the protection of the persons concerned and avoid creating confusion in the minds of controllers of the file.

46. Several replies wisely observe that there is no point in including definitions of additional players if a particular legal regime setting out obligations is attached to these new players.

47. Several replies state that it is essential to add a definition of sub-contractor. The Italian Garante per la protezione dei dati personali further observes that the need to introduce such a definition has already been felt in several Council of Europe instruments (Recommendation 2002(9) on data protection in the insurance sector and Recommendation 2010(13) on profiling).

48. By contrast, Privacy International considers that the concept of sub-contractor is no longer useful, since sub-contractors in fact have to comply with so many obligations in respect of security and respect for privacy that their role becomes very hard to identify. There is a problem in asking controllers to take responsibility for privacy and security measures when they are in reality entirely dependent on the contractual conditions laid down by service providers (especially cloud) who are not subject to the regulations.

49. The German Insurance Association calls for a flexible definition here, permitting the parent company, depending on circumstances, to be appointed as sub-contractor by a company in the group, though in such cases there should be limits on recognising the right to issue instructions in accordance with existing law.

50. The AEDH proposes that a distinction be made in the case of service providers processing data on behalf of the data controller of the file but enjoying clear autonomy in the provision of the service, so that they would wear the two hats – that of data controller of the file and that of sub-contractor. In this hypothesis one could introduce the concept of "person entrusted" with processing ("personne chargée"): where the sub-contractor acts strictly on behalf of and on the instructions of the data controller of the file and is not responsible as controller of the file, the person entrusted with processing could be regarded as bearing part of the responsibility, either jointly or in full.

51. In the opinion of the ICUK, the mere distinction between controller of the file and sub-contractor no longer reflects the complex relationship which exists between organisations processing personal data. The model definitions in Directive 95/46 correspond to a passive sub-contractor acting only on the instructions of the controller, whereas in reality the person regarded as sub-contractor may have considerable influence on the manner in which processing takes place and may, in many respects, act as a controller of the file. The CNIL considers that this situation, in which actual day-to-day processing of data is in effect, increasingly, in the hands of the sub-contractor, not of the data controller of the file, ultimately requires that this category of player be defined. That body believes that consistency with the definition in the directive stating that it is the organisation acting on behalf of the data controller of the file is necessary. It also argues that the rules governing the sub-contractor's responsibility should be more fully harmonised and regulated at European level.

52. Regarding the addition of a definition of “manufacturer of technical equipment”, some contributors such as the European Banking Association see this as a good idea, while the AEDH regards it as quite essential, whether the equipment in question is hardware or software. The Cyberspace Law and Policy Centre (Australia), in common with the Cyprus Commissioner for Personal Data Protection and the CLSR-IAITL-ILAWS consortium, observe that this will prove to be necessary if rules on “Privacy by Design” are introduced – which, unlike the others, the Cypriot authority would not welcome.

53. The Italian Garante has a less clear-cut approach: it believes that it would undoubtedly be useful to set out the guarantees which should be offered by any additional entity which plays any part in processing (such as a manufacturer of technical equipment), while placing the legal obligation to check that these guarantees are respected on the data controller of the file.

54. Privacy International, on the other hand, thinks it would not be wise to define equipment manufacturers beyond a specific risk to privacy and a security context. The Direcçao Geral da Politica de Justiça in Portugal is also opposed to the inclusion of this concept, which it does not find helpful.

PROTECTION PRINCIPLES

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection whenever possible.

55. Many contributors point out that the proportionality principle is already contained in Article 5 of the Convention. They accordingly restrict the application of this principle to data which must be relevant and not excessive.

56. Other contributors think that the inclusion of the principles of proportionality and minimisation or limitation of data collection in the protection principles should be recommended, and some argue that these principles should be explicitly stated, not merely implied. The explicit formulation of these principles would make it possible to define their scope better and more precisely. In particular, it would make it possible to stipulate that the proportionality principle applies to all operations, not just to data collection (Cyprus Commissioner). In other words, the proportionality principle linked to the purpose of each processing operation (Garante) or the criterion in respect of the non-excessive character of an entire private data processing project relative to the fundamental freedoms and rights in question must be respected, in addition to the need to minimise the data processed (AEDH). Similarly, the AEDH says that the principle of data minimisation must not replace that of proportionality because the latter must go beyond data alone.

57. Some contributors are strongly in favour of including these principles, which they see as very important (CLPC, Australia; APEP - Spanish Professional Association for Privacy; Czech Office for Personal Data Protection; CLSR-IAITL-ILAWS; Italian Garante).

58. Morpho-Groupe Safran (identification technologies), which regards the proportionality principle as one “which seeks to strike a balance between the processing of data and the aim pursued”, is mistrustful of the subjective approach implied by the application of this principle. That subjectivity results in divergences between national data protection authorities in the acceptance or otherwise of an industrial product or device. Consequently, they would like this principle, if it is set forth in the Convention, to be accompanied by

objective provisions such as to encourage recourse to labelling/certification procedures based on precise criteria which the manufacturer would have to respect in order to develop his products.

59. The GDD (German data protection and data security association) considers that certain advantages should be granted to organisations using pseudonyms rather than data directly linked to persons.

60. ARD and ZDF (radio and television) consider that, whereas users of traditional media have always enjoyed complete anonymity, that is no longer true of services provided via the Internet. Consequently, they strongly support the principle of strictly limiting data collection to the aim pursued.

61. CEA Insurers of Europe asks for data minimisation to be presented as an objective, not as an obligation.

8. Should the question of consent be considered in close connection with the principle of transparency and obligation to inform, or as a necessary condition for fair and lawful processing, to be met before any other step?

62. Several contributors believe that the role of consent as the legal basis for data processing should be qualified. In any case, it ought not to be the sole basis. Some believe it should not be presented at all as a condition to be met for processing to be legal and fair. In many cases the persons who give consent do not realise what they are agreeing to. Consent is neither a guarantee of protection for the persons concerned nor a practicable solution for data controllers of the file, for whom it may constitute a disproportionate burden (for example in the worlds of marketing or insurance).

63. Quality of consent causes huge apprehension. There are references to problems of genuinely free consent, and problems arising from the form of consent increasingly employed.

64. On this point, the GDD (German data protection and data security association) considers that the relevant German law offers consumers good protection. It stipulates that if consent is given in a form other than writing, the data controller of the file must give written confirmation of the substance of that consent to the person concerned, unless consent was given in electronic form, in which case the controller must keep a record of the consent to which the person concerned must have access and which he/she can revoke at any time with future effect.

65. The CLPC (Australia) proposes the example of the Canadian law governing protection of privacy in the private sector (PPIDEPA). There is a particularly interesting proposed amendment to that legislation: “An individual’s consent is valid only if it may reasonably be expected that the individual understands the nature, purpose and consequences of the collection, utilisation or disclosure of the personal information to which he/she consents”. The CLPC says that, if the concept of consent is introduced, consent must be expressly defined as free, informed and revocable and not linked to other consents. There should also be a general principle stating that, where true consent is a realistic option, it should constitute the main basis of legitimate processing, which would be consistent with the overall aim of transparency in the processing of personal data.

66. The US Federal Trade Commission points out that denying the persons concerned the choice of practices which are straightforward for consumers makes it possible to restore meaning to choices about more problematic practices (such as transferring their data to third parties who have no connection with the purpose of the data processing).

67. Many contributors stress that consent must be linked to transparency. In the opinion of Privacy International, transparency must even prevail over consent, in the sense that prime importance must attach to clear, easily found and easily understood information provided for the persons concerned before judging whether processing is authorised (and then based on opt-out rather than opt-in). Furthermore, other contributors stress that one should be wary of long and rarely read privacy policies. For the APEP - Spanish Professional Association for Privacy believes that a general duty of information should be established in order to ensure transparency.

68. The European Newspaper Publishers Association and the FAEP (European Federation of Magazine Publishers) point out that an exception for the media would be needed for any question of consent, whether in terms of an obligation of transparency and information or as a necessary condition for fair, lawful processing. This must apply to all their activities - archiving of articles, recording of research material for preparation of articles, everyday collection of news, investigation, verification, publishing, deletion, whether or not this leads to publication of the material, and lastly subsequent publication and communication.

9. Should the legitimacy of processing be addressed by Convention 108 as Directive 95/46 does in its Article 7?

69. Some contributors fear that the introduction of such a list would reduce the flexibility of the Convention (TechAmerica). The Garante, like the Cyprus Commissioner for Personal Data Protection and CEA Insurers of Europe, emphasises that one should avoid modelling the Convention's principles too closely on those set out in Directive 95/46, since that would mean introducing excessively detailed provisions into the Convention. This concern is shared by the German Insurance Association, which argues in favour of a high degree of abstraction in the Convention, especially bearing in mind third countries' wish to accede. Similarly, the FEDMA states that this ought not to appear in the substance of an international convention. It would be more appropriate to a directive.

70. Privacy International is more radical still, considering that such an approach to legitimacy is redundant and pointless. Dishonest aims are obviously not legitimate, unless they are (sic) (hypothesis of aiming to deceive a fraudster, for example). As they see it, the list of reasons for legitimising processing set out in the directive has created a playground for lawyers, strewn with pitfalls. Finally, they fear that a list of positive bases for carrying out data processing will inevitably be incomplete. They see the combination of the requirement of fairness and lawfulness (= not "unlawful"), coupled with the other general principles of proportionality, data minimisation and non-intrusive collection as appropriate criteria. These last points are restated word for word by the Cyberspace Law and Policy Centre and the CLSR-IAITL-ILAWS consortium.

71. At the other end of the spectrum, some contributors find it opportune, useful, and indeed important, to include such a list of legitimate bases, out of a concern for consistency with European Union law or a concern for clarity for those in the field who need to have clear parameters on lawful processing (AEDH, European Privacy Association, European Banking Federation, Data Industry Platform, the Czech Office for Personal Data Protection, the Bulgarian Personal Data Protection Commission, the Portuguese Direcçao Geral da Politica

de Justiça, the Ministry of Justice of the United Kingdom). EFAMRO and ESOMAR are in favour of the introduction of a basis for legitimate data processing into the Convention, but not of an exhaustive list of legitimate bases.

10. Convention 108 does not expressly mention the need for compatibility between the use made of data and the initial purpose of collection. In today's context, personal data are commonly used for purposes that go far beyond what may have been initially foreseen, hence the issue of compatibility.

72. Few contributors understood the pertinence of this question, since Article 5 of the Convention already requires that data should not be used in a manner that is incompatible with the purposes. For many people, therefore, the question has already been settled.

73. However, some of them observe that the question of later processing arises more and more often, mainly owing to the mass availability of data on the Net, and should be dealt with.

74. The European Privacy Association believes that the main issue is not to mention the requirement of compatibility with purpose but rather to extend the scope of Article 5 (b) of the Convention to all data processing. They suggest taking the text of Article 6.1 b) of the directive as a model.

75. It is pointed out that later processing for historical, statistical or scientific purposes should be permitted. EFAMRO and ESOMAR call for "market, social and opinion research" not to be regarded as incompatible with the initial purpose of data processing, and this is already allowed by Recommendation R(97)18. These bodies call for the inclusion in the Convention of a provision similar to Article 6 paragraph 1 b) of Directive 95/46.

76. CEA Insurers of Europe ask that it be possible to change the purpose in cases where the new purpose can be legally justified.

77. Matthias Pocs, considering this question from the standpoint of the police where it arises in an acute form, proposes (and supports his proposal with factual arguments) that Convention 108 should provide for the processing of personal data for purposes other than the specified ones to be prohibited if the person concerned is suspected of a lesser or moderately serious offence, but permitted if the person concerned is suspected of a serious criminal offence and adequate guarantees against infringements of human dignity are given.

11. Special categories of data which enjoy enhanced protection are defined very widely, which could lead to excessive application of this restrictive regime : are the data sensitive or their processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

78. **Relevance of a category of sensitive data:** the UK Ministry of Justice requests the Consultative Committee to reflect on the possibility of sensitive data being linked to their use rather than simply extending the list of sensitive data (he refers to the example of a photograph which might be regarded as biometric data, and where there is a huge difference between its being attached to a library ticket and being taken at the door of a treatment centre for drug addicts). This viewpoint is shared by several contributors for whom data sensitivity is essentially a matter of context.

79. In the view of several contributors, the proportionality principle offers adequate safeguards for these data. One could leave the present list as it stands and rely on the proportionality principle to counter the dangers arising from other data.

80. The Italian Garante considers that the greater protection afforded to data in the present list, which broadly corresponds to the categories protected by international instruments to combat discrimination, should be left untouched. On the other hand, one might envisage a "functional" criterion whereby additional categories of data could be classed as sensitive because of the context and/or purpose and/or processing mechanisms. In these cases, such data would be subject to enhanced protection. One could also envisage circumstances and data categories being determined and regularly updated by flexible tools not involving amendments to the Convention. This viewpoint accords with that of the Data Protection Commissioner for Mauritius, who considers that a distinction could be drawn between data that are sensitive by reason of their nature and data that are sensitive by reason of the processing applied to them (such as a name or photograph revealing racial origin). The APEP also emphasises that any prejudice which might result from the processing of these sensitive data depends on the purpose of processing.

81. **The list of sensitive data:** several contributors wonder what is covered by the concept of "biological" data. Some consider that it should not cover such characteristics as gender or age, which are apparent to everybody.

82. Some replies suggest that genetic and biometric data be added to the list.

83. Morpho-Groupe Safran, a company specialising in identification and applications using biometry, points out that, unlike names, fingerprints give no clue as to ethnic origin or supposed religious allegiance. Moreover, a name is the key giving access to masses of information on the Internet via search engines, as distinct from fingerprints. So the company wonders why biometric data should be subject to more binding legal rules when they provide less information than people's names. Moreover, Safran wonders what should be done about "voice prints" obtained from electronic messaging and stored on servers to build biometric databases. Should these data enjoy different legal rules from fingerprints, and on what basis? Safran gives information about genetic fingerprints as distinct from genetic data and points out that in some situations the use of biometric data such as iris recognition or digital fingerprints, if rendered anonymous, makes it possible to decide whether an individual may or may not be granted a right (to enter, for example) without his/her identity being disclosed.

84. The APEP - Spanish Professional Association for Privacy shares this reluctance to have biometric data regarded as sensitive, since in principle these data do not relate to information about health. This association also finds it difficult to class (national) identification numbers as sensitive.

85. In the view of the AEDH, apart from biological information needed in a medical context, the question arises whether, in the name of protection of the human person, information such as national identity numbers and biological or biometric data which serve as reliable identifiers for a person should actually exist at all, especially when they relate to every member of a community, not just to certain persons for particular reasons of public necessity. This organisation regards the existence of such information systems as highly dangerous in all exceptional circumstances (regimes becoming undemocratic). Furthermore, these systems which physically link persons to the state breach the social contract and stem from the idea that every citizen is a potential delinquent, which is unacceptable. So data of this kind must not be made subject to a system of enhanced

protection in order to prevent discrimination. What is needed is a system of prohibition which can be lifted in accordance with the criteria set out in Article 9 of the Convention.

86. The CNIL proposes referring to ethnic origin rather than racial origin.

87. Several contributors request that, if consideration is given to extending the list of sensitive data, this be preceded by an impact study.

88. Regarding the **rules governing these data**, the CNIL requests that they be more detailed, because the contents of the Convention as it now stands lack precision. It also says that an exception should be made for statistical processing and scientific research.

89. EFAMRO and ESOMAR would welcome clarification on what the term "sensitive data" covers. They also point out that insisting on recourse to an authority before sensitive data are allowed to be processed places too heavy a burden and too great a barrier on the research sector.

90. The European Newspaper Publishers Association and the FAEP call for an exemption for the press sector from the strict rules on sensitive data.

12. Specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, what are the issues that should be addressed in such provisions?

91. Data concerning minors should not fall into the sensitive data category, since the person concerned by the data cannot constitute a sensitivity criterion (Bulgarian Personal Data Protection Commission).

92. That being said, it is important to provide for special conditions for the protection of minors because of their vulnerability. Several contributors consider this necessary. The APEP - Spanish Professional Association for Privacy observes that there is unanimous agreement that children deserve specific protection, but the discussion is about the relevant age to be taken into account, whether and from what point parental control infringes the child's right to privacy, who is to grant parental authority, etc. Specific obligations should be imposed in cases where children are the target of the processing. The specific protection regime should be based on obligations as to means, not results.

93. The Federal Trade Commission outlines the specific American on-line system of child protection (the Children's Online Privacy Protection Act), which lays down a series of rules designed to protect children below the age of 13. These rules are currently being reviewed to ensure that they continue to offer an adequate response to changing technologies, and especially to practices involving a boom in the use of mobile terminals and interactive games by children.

94. By contrast, many contributors do not believe that a particular protection regime has its place in the Convention. Specific rules are set down in other instruments. A recommendation would probably be more appropriate here. Alternatively, the explanatory report could make it clear that the introduction of the principles of proportionality and minimisation is an adequate response to the concerns about children - and other vulnerable groups (CLPC, Australia).

95. This is all the more so because there are difficulties in harmonising the meaning of “minor”, “minor with capacity of discernment” and “minor with capacity to express consent”. Just as there are difficulties in verifying and ensuring compliance with age limits on the Internet.

96. Lastly, several contributors point out that there are other categories of vulnerable persons apart from minors.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

97. Several contributors think it desirable to provide for such a right to be informed about security breaches, applicable across the board to all sectors. The CLPC, together with the CLSR-IAITL-ILAWS consortium and Privacy International, believe that this right should not appear as part of the principle of security but as a separate principle.

98. Most replies state that is is imperative for the limits of such a right to be clearly indicated. The European Privacy Association says that the text should stipulate when the information is to be given, to whom and in what manner. TechAmerica Europe proposes markers to define this obligation. The Data Protection Commission of Senegal considers that there should be an obligation to inform the public supervisory authorities but not the persons concerned, who are in any case powerless in the face of infringements. The German Insurance Association offers the benefit of German experience: in 2009, an amendment to German data protection legislation introduced a duty to inform in cases of unauthorised access to data. That obligation applies where particularly sensitive data are concerned and where there is a real risk of serious infringement of the legitimate rights or interests of the persons concerned. To their knowledge, this rule has proved positive in practice. They stress the need to limit this kind of obligation strictly to cases of real risk to the persons concerned. Morpho-Groupe Safran does not deal with hypothetical case of unauthorised access but considers that this right to be informed of security breaches should be expressly justified by the need to protect identity and limit the risks of usurpation of identity.

99. However, several contributors fear that it would not be possible to introduce such a right without transforming the Convention into an unduly detailed instrument going beyond general principles.

100. Some contributors, such as the Czech Office for Personal Data Protection, are opposed to the idea of introducing this right, believing that the question is sufficiently dealt with in the European directive. The Data Industry Platform fears that additional burdens may be placed on agencies in the field without giving the persons concerned a higher level of protection. This group of signatories appreciates the importance of security and the need to create confidence among the persons concerned and data controllers. Thus they are sympathetic to the concept to the extent that it is an incentive to security. However, they consider that the question would be more suitably addressed by instruments of self-regulation. FEDMA and the European Banking Federation express exactly the same fears and convictions. EMOTA (European E-commerce and Mail Order Trade Association) also shares these misgivings.

101. Several contributors state that in any event one should not fall for an “overly prescriptive” wording, which would impose an excessive burden and at the same time rob the measure of its effect, making notification of those concerned routine.

102. Garante sees the question of security as crucial, especially in the context of cloud computing. Article 7 of the Convention should be revised. It would be appropriate to consider extending the concept of security to include the security of data transmission networks, over and above the physical security of the premises where data are kept.

103. Similarly, Privacy International recommends that the passive interpretation of "data security" be replaced by a positive obligation to design systems in such a way as to minimise the risk to privacy - for example ex ante minimisation. So one must not only seek to protect the data processed, but to minimise the risk to privacy throughout the system.

14. There are special risks arising from the use of traffic and location data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data ?

104. There are contrasting replies to this question.

105. Some contributors think it would be desirable to provide for a stronger protection regime for processing aimed at locating individuals spatially.

106. The AEDH observes that traffic data affect freedom of communication, and location data freedom to come and go. Because of this interference with freedoms, a more stringent regime should be applied to them. The same is true of requests made on a search engine, which affect freedom of information. Similarly, Privacy International sees traffic and location data as data concerning social relations and impinging on freedom of association and the right to associate freely, in a private, unobserved way. Consequently, Privacy International takes the view that such data should constitute a special category and be considered as inherently "toxic" to privacy.

107. The CNIL points out that placing these data in the sensitive category could well place a check on certain technical innovations. It would be better to add clearly distinctive protection elements to the Convention, designed in particular to require appropriate guarantees for "personal data used in processing for the purpose of revealing an individual's spatial position". That would make it possible to exclude data which may reveal an individual's position but whose purpose is not to do so, while not placing these data in the special categories provided for in Article 6 of the Convention. A third possible option suggested by the CNIL would be to propose a specific right not to be geo-located.

108. Other contributors see no need to provide for specific rules. The British Information Commissioner likewise believes that sensitivity relates more to data processing and t he effects it may have on individuals rather than to the nature of the data processed.

109. The CLPC, echoed by the CIPPIC, argues that there should be no need for a particular regime if care is taken to ensure that traffic and location data are brought within the definition of personal data, stating explicitly that "personal data" covers any information which permits or facilitates communication with a person on an individualised basis, whether or not that information conforms to the present definition of personal data.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full compliance with data protection rules be introduced?

110. Most of those who replied to this question favour the idea of introducing an obligation to comply with the accountability principle as a guarantee of improving the protection afforded. Accountability mechanisms should be clearly defined; they should not be excessive and should be implemented by all signatories in the same way.

111. Privacy International, in common with the CLSR-IAITL-ILAWS consortium, advises caution with regard to the suggestion made by some contributors that accountability should be seen as an alternative to the requirement of respect for the protection rules. Accountability must not become an alternative to restrictions on the export of data. This organisation is concerned about the consequences, or rather the absence of consequences, which accountability failures may have if this principle is interpreted loosely.

112. The APEP - Spanish Professional Association for Privacy considers that a "reward" (for example a lesser penalty) should go to file controllers who are "accountable" in cases where data protection infringements are due solely to an exceptional error.

113. TechAmerica Europe supports the introduction of an accountability principle if it is defined in an ex post approach based on the application of the rules rather than an ex ante approach based on conformity with the rules. In an ex-post system, organisations are responsible for what they do with data wherever the latter go, instead of simply trying to comply with the law. This has implications for the way in which the organisation sees data protection, the way in which it implements it and the way in which it oversees it.

114. Some contributors are opposed to the introduction of an obligation to demonstrate compliance because it would constitute a burden, especially for small and medium-sized enterprises.

16. Should the principle of "privacy by design", which aims at addressing data protection concerns at the stage of conception of a product, service or information system, be introduced?

115. In view of the fact that the principle of privacy by design has been proclaimed by several bodies, was the subject of a resolution adopted by the 32nd international conference of data protection authorities and is being taken into account by the European Commission in the framework of its revision of Directive 95/46, it seems logical that this principle should also be enshrined in Convention 108 (Safran).

116. Other contributors share the belief that this principle should be expressly encouraged, even if it will be difficult to give it operational effect by way of a specific rule (Privacy International, British Ministry of Justice, CNIL, Senegal's Data Protection Commission). Or else they say it is welcome, but the way in which it is to be defined and implemented must be clarified before it can really be advocated (TechAmerica Europe). Introduction of the privacy by design principle would foster a proactive approach to protection rather than reliance solely on corrective measures

(Garante). As the AEDH sees it, the obligation to apply protection principles from the stage of design of equipment and applications could be simply stated in the text without necessarily employing a “marketing vocabulary” such as that of privacy by design. The ICUK observes that this principle is already implied by the existing protection principles. However, an explicit requirement would have the advantage of sending a clear signal to data systems designers, those who supply them and those who operate them.

117. The Italian Garante points out, however, that the effectiveness of the principle cannot be guaranteed except by specifying how its impact on particular processing operations can or should be measured and by whom, in the light of specific technological provisions.

118. The Bulgarian Personal Data Protection Commission considers that, for this principle to be applied effectively, data controllers should be required to carry out assessments of the risk to privacy in data processing. Privacy International also favours an obligation to carry out a privacy impact assessment for major projects.

119. The last-mentioned organisation says that the simplest way of expressing the principle of privacy by design is to state that, if scientific discoveries show that a service can be offered in practice by a method which is more respectful of privacy, the adoption of advanced protection technologies may be made mandatory. It also observes that one must not be influenced by the false rhetoric of lobbyists who attempt to confine privacy by design to a mere state of mind, an awareness of the principles of data protection when commercial products are designed, “immunising” the concept against any technical obligations.

120. According to TechAmerica, privacy by design is a process which organisations should follow at the start of a project and re-assess at regular intervals in order to check that data protection and security measures are still appropriate. It is important that, whatever requirement is laid down in the legal instrument, it remains a matter of procedures, not technology. The AFME BBA (banking) considers that the wording of the principle must be high-level and not prescriptive with regard to the measures to be adopted.

121. For its part, the FTC recommends in its report designed to improve protection of privacy in the United States that firms should adopt a privacy by design approach. This means constructing privacy protection mechanisms as part of day-to-day business practices. This protection includes the provision of reasonable security for personal data, limits on data collection to necessary data only and conservation of data for a limited period of time. On the basis of its own experience, the FTC encourages the Consultative Committee under Convention 108 to adapt the concept of adaptability when dealing with the question of privacy by design.

RIGHTS – OBLIGATIONS

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

122. Adding the right of access to the origin of the data and to the logic underlying processing is absolutely necessary in the opinion of the AEDH, very important in the opinion of the Bulgarian Commission, and achieves consistency with the European Union rules in that of the ICUK and the British Ministry of Justice: the CIPPIC and the Garante consider it necessary in the growing context of the complex IT models on which criteria and assumptions are made, with potentially negative effects on individual privacy; and other replies state simply that it must be envisaged. The European Privacy Association fears, however, that given the involvement of large numbers of players in automated processing today, the obligation of transparency of processing - which the association supports - may not be achievable without excessive cost.

123. The AFME BBA (banking) supports the move provided it does not go beyond the right introduced by Directive 95/46, in so far as it would not mean obliging the persons concerned to keep information about data sources and entails only the duty to transmit the information about sources where they are known. On the question of keeping information about data sources, the reply of the German Insurance Association states that German data protection law contains an obligation to keep data about sources and recipients of data for a period of two years.

124. Portugal's Direcçao Geral da Politica de Justiça considers that access to processing logic requires that the data subject demonstrate an interest and must be limited to the extent strictly necessary to satisfy that interest. Thus access to processing logic must not translate into unwarranted disclosure of business secrets.

125. CEA Insurers of Europe points out that some requests for access are frivolous and seek only to check the processing of data rather than verify the accuracy of the data processed. Consequently, this group believes that the right of access should be limited and that introduction into Convention 108 of a right of access to the logic should not be envisaged. This stance is shared by the Data Industry Platform, which is anxious to preserve commercial secrets, companies' competitiveness and their intellectual property. Internal predictive analysis techniques are of crucial value to the business world and should not be disclosed to third parties. The FEDMA shares this view.

126. Privacy International considers that the protection secured to intellectual property (patents) permits transparency without fear. In exceptional cases where secrecy must be preserved, the supervisory authorities should be allowed confidential access to the algorithms in order to check their legitimacy.

127. The FTC provides information about cases in the United States in which consumers are entitled to obtain information from firms which have taken action with negative consequences for them. One case illustrates the possibility of achieving a compromise between transparency and business secrecy: credit reporting agencies are not required to reveal exactly how credit ratings are calculated, but the disclosure required of them must include the range of possible credit ratings in the assessment model and the key factors negatively affecting the consumer's rating.

128. The CNIL insists that the exercise of access, opposition, correction and blocking rights must be free of charge.

129. The Garante invites the Committee to reflect, where technologies based on cloud computing are concerned, on the introduction of a right to know the physical location and the country where data are kept or where distribution servers are situated.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The link between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect for, and exercise of, this right.

The right of opposition

130. The right of opposition is justified in the opinion of most contributors, but not in all circumstances. One might consider introducing this right into the Convention for reasons of consistency with the directive. Some replies (others disagree) state that this right should be granted even where processing is based on consent, if it is admitted that consent can be revoked in all circumstances.

131. A similar right exists in Canadian law (PIPEDA), permitting the persons concerned to object by way of opt-out to collection, utilisation and communication of personal data for non-necessary purposes.

132. The Bulgarian Commission stresses that the link between the right of opposition and the right of oblivion consists in the right of opposition being exercised taking account of the purpose of processing, whereas the right of oblivion is exercised irrespective of the justification of processing in relation to purpose.

The right of oblivion

133. The following picture emerges from most of the replies. The right of oblivion may be particularly indicated and practicable in certain circumstances (mainly in the framework of social networks). Otherwise it is problematic in several respects:

134. - It conflicts with the rights, interests and freedoms of others, in particular freedom of expression, freedom of the press (it impinges on the conservation of full archives), the duty of memory, business continuity, management of employee files, the duty to keep evidence, etc. It is a hindrance to historical research. It may also hamper the provision of certain services such as medical treatment in cases where the medical history of the person concerned is not known;

135. - It is difficult to implement once the data have been rendered public on the Internet.

136. In the opinion of the APEP, the right of oblivion is not a sub-category of the right of opposition in so far as, unlike the latter, it has retroactive effect. So the question is whether individuals must be responsible sine die for their past actions and whether it is desirable for them to have the right to rewrite their past, and consequently that of others.

137. Some contributors favour its inclusion in the Convention. Others - more numerous - consider that further reflection is needed before a decision is taken, giving thought in particular to the practical obstacles to its implementation and clarifying the cost and practical implications of including such a right. Clarification should be forthcoming about the data which would be the subject of such a right of erasure: if it concerns data obtained from the person concerned, does it also cover analytical data or meta-data created by the data controller of the file? It is stressed that the right of oblivion cannot be absolute in any case. The Data Industry Platform points out that this right should not appear in a list of general principles tested over a period of time. On this point, it is supported by the Garante, which does not look favourably on the inclusion of so controversial a right in the Convention.

138. The Data Industry Platform argues that, if the inclusion of this right were to be envisaged, it should imperatively be limited to services based on data which the individuals concerned have themselves supplied and which are made accessible to third parties as part of the service. Some other replies echo this standpoint, limiting the scope of such a right to social networks.

139. Yet others, lastly, regard this right as utterly unrealistic both technically and legally (EMOTA - European E-commerce and Mail Order Trade Association) or as having disastrous consequences for publishers and freedom of expression (European Newspaper Publishers Association et European Federation of Magazine Publishers) and say it should be dismissed absolutely (a stance taken especially by the various contributors from the press sector).

19. Should there be a right guaranteeing the confidentiality and integrity of information systems?

140. It should be noted that many contributors omitted to reply to this question.

141. Some replies were positive, but in most cases not backed up by arguments. Among them, the Garante stands out by stating that, in its view, the rights concerned in this question, like those covered by the following questions, are those which most justify the Convention's list of rights and general principles.

142. However, other contributors fail to see on what grounds the confidentiality and integrity of systems should be the subject of a right, instead of strengthening the security constraints set out in Article 7. The extra value of such a right remains to be demonstrated and should be set against the risk of dilution and loss of legibility of the rights enshrined in the Convention.

143. The Czech Office for Personal Data Protection observes that the guarantee of confidentiality relates to the obligations on controllers, not to the rights.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

144. Some contributors agree with the idea of introducing such a right, subject to reasonable exceptions.

145. The Garante, commenting on the three rights referred to in questions 19, 20 and 21, considers this right essential.

146. Other contributors say that further consideration is called for.

147. The AEDH and the Data Industry Platform think that application of the general protection principles (in particular the prohibition on keeping data for longer than the aim requires) provides a satisfactory answer. Similarly, the CIPPIC believes that the principles of "confidentiality, privacy and accuracy" ensure this right. The CLPC also believes that there is no need to lay down a separate right if personal data are defined in such a way as to encompass information about an individual's communications, location or behaviour.

148. The European Privacy Association suggests that, rather than a right not to be tracked, there should be an option not to be tracked. The persons concerned should be informed about tracking practices and be given the option and the technical means of refusing to be traced/located. The APEP also refers to an option to be made available to the persons concerned, rejecting the idea of a prohibition. Tracking technologies are not bad in themselves, but certain uses must be limited in cases where privacy must prevail. The association argues that the tracing of Alzheimer patients, lost luggage, vehicles, children or animals should not be prevented. Moreover, the concept of tracking is not limited to RFID but also covers cookies in particular.

149. Several contributors observe that a right must not be based on a targeted technology, which would run counter to the aim of preserving the technologically neutral character of the Convention.

150. Nor must legislation stand in the way of all progress and all technical development in this matter.

21. Should users of information and communication technologies have a right to remain anonymous?

151. The Garante, commenting on the three rights referred to in questions 19, 20 and 21, considers this right essential.

152. The AEDH observes that social life is based on a dialectic of identification and anonymity that is no longer found in present-day conditions where, for example, consultation of public information leaves identifying traces, just like any form of payment, since there is no electronic currency equivalent to banknotes. This constitutes a "basic defect". In such a context, everything rests on the length of time for which data collected are kept. In this association's opinion, there should be social and technical guarantees of the right to anonymity.

153. Similarly, the CIPPIC is of the opinion that anonymity is a right which deserves to be separately formulated and protected. The ability to act anonymously is central to the

protection of privacy in public and semi-public space. It points out that the wording of this principle as proposed by the CLPC on the basis of the provisions of Australian privacy legislation is interesting. The CLPC suggests the following wording: "Individuals must have the option of not identifying themselves when dealing with an entity, or of using a pseudonym, except where there is a legal obligation of identification or where it is not practicable for the entity to deal with individuals who are not identified or who use a pseudonym".

154. Several contributors are in favour of a right to anonymity provided the law is not infringed.

155. Other contributors, on the other hand, do not think there should be a right to anonymity because it could lead to an increase in fraud and crime, it being difficult if not impossible to find the perpetrators. The European Privacy Association is opposed to a generic right to be absolutely anonymous when using ICTs, which would conflict with practical needs (individuals need information about their use of ICTs, at least for the purpose of billing such use) and for the requirements of law enforcement bodies. However, this information must be protected against misuse. As the EPA sees it, this protection is already secured by the Convention. The APEP quotes the example of an employer legitimately overseeing the actions of his employees for which he will be held responsible.

156. The Data Industry Platform, contrary to the contributors mentioned above, inquires whether the off-line community really knows about default mechanisms or a right to remain anonymous in normal circumstances. For example, the staff of a public library know that library's users and their reading preferences. The group sees no reason to draw a distinction between the on-line community and the off-line one.

22. Should Convention 108 address the question how to strike the right balance between protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

157. In general yes, but replies differ somewhat about the manner of doing so.

158. The European Privacy Association believes that the - decisive - link which exists between the right of data protection and freedom of expression should be defined. A link with Article 10 of the European Convention on Human Rights could be addressed in the preamble to Convention 108.

159. In the opinion of the European Broadcasting Union (EBU-UER), Article 9. 2. b) together with paragraph 58 of the explanatory report is not sufficient and should be explicitly strengthened in order to grant a clear exemption from the application of certain data protection rules to journalistic activities, especially in the audio-visual field. That organisation accordingly proposes amending Article 9 by the addition of a paragraph reading: "9. 2. c) - protect the processing of personal data carried out solely for journalistic purposes". The EBU regards such an amendment as vital in order to preserve the freedom of the media, investigative journalism and the confidentiality of journalists' sources.

160. The Centre for Socio-Legal Studies proposes drafting a new provision requiring the parties to strike a balance between the fundamental interest of freedom of expression and the values which data protection seeks to uphold. The provision

should also mention the need to adopt broad, but not absolute, exemptions from the protection rules for these activities. As for the possibility of expressly stipulating minimum exemptions in accordance with Article 10 of the European Convention on Human Rights, this requires fuller consideration. The explanatory report should state explicitly that this provision to safeguard freedom of expression is not limited to the press. In principle, it should hold good for any form of public expression.

161. The APEP considers that any regulations in this field must be flexible: they must provide criteria to serve as guidelines, but not themselves conduct a predetermined general assessment. By contrast, the CNIL considers that similar provisions to those in the French law on data processing and freedoms could be incorporated into the Convention. That body thinks it would be helpful to state at the European level the exemptions and derogations from which processing might benefit. In the CLPC's opinion, it would not be appropriate for the Convention itself to weigh up all aspects of these conflicting interests, but it ought nonetheless to contain a provision recognising the public interest of freedom of expression.

162. The AEDH observes that even in Europe there is no consensus on the limits to be set on freedom of expression in the name of protection of privacy. That association therefore advocates an initiative aimed at bringing standpoints and procedures closer together. That initiative should be taken in the Council of Europe, possibly in conjunction with UNESCO.

163. The ICUK wonders where the line should be drawn in the age of blogging. Up to what point will supervisory authorities be required to regulate individuals' behaviour on line?

164. The Italian Garante is opposed to the inclusion in the Convention of provisions which might prove less flexible than what emerges from the case-law of the European Court of Human Rights in reconciling the two rights, or which might fail to strike the same balance. As for the questions linked specifically to Web 2.0, it seems premature to lay down specific rules.

SANCTIONS AND REMEDIES

23. Should class actions be introduced into the Convention? Should more scope be given to alternative dispute resolution mechanisms?

165. **Class actions**. Various contributors regard the introduction of class actions as desirable, either in certain specific contexts[125] or generally, and say that this should be mentioned in the Convention.[126] Others point out that, on the contrary, the general character of the Convention does not lend itself to this.[127] Similarly, the question of sanctions and remedies ought more broadly to fall within the scope of domestic law rather than that of the Convention.[128] Some replies also observe that the class action debate should take place in a broader context than that of data protection.[129]

166. Apart from these methodological objections, there are some misgivings about the general introduction of class actions. Some replies state that they are not needed,[130] or even that they are inappropriate.[131] It is argued that class actions are of no interest where the person concerned already has the benefit of protection mechanisms to rely on in the exercise of his/her rights[132] (eg. data protection authorities). Class actions would be useful only when other remedies are unreliable[133] or ineffective, in short where recourse to this remedy would be of direct practical interest.[134] Others note that data protection disputes are specific to individuals and would therefore not lend themselves to class actions.[135] Yet other contributors point to the risk that class actions would permit the harmful use of data

[125] Opinion of the CIPPIC.

[126] Opinion of the Czech Republic's Office for Personal Data Protection; opinion of the Mauritius Data Protection Commissioner; opinion of the Ukrainian Ministry of Justice; opinion of the United Kingdom Information Commissioner's Office; opinion of the Direccao Geral da Politica de Justica.

[127] Opinion of the EPA; opinion of the Italian Garante per la protezione dei dati personali. Various contributors stress that this is a matter for domestic law; see, for example, the opinion of the Lithuanian State Data Protection Inspectorate.

[128] Opinion of the CEA.

[129] Opinion of the EBF.

[130] Opinion of the Data Industry Platform.

[131] Opinion of the ENPA-FAEP.

[132] Opinion of the German Insurance Association. See also the opinion of TechAmerica Europe, which also emphasises that the extent of public demand for class actions should be assessed.

[133] Opinion of the Italian Garante per la protezione dei dati personali.

[134] Opinion of the UK Ministry of Justice.

[135] Opinion of the FEDMA.

protection rules.[136] Dealing with class actions at this stage would also create uncertainty.[137]

167. However that may be, the Convention could nonetheless emphasise the benefits and value of class actions if it did ultimately deal with the question of remedies.[138] And if recourse to class actions were envisaged, it would be above all important to assess the impact they might have in the European context.[139]

168. **ADR.** Some contributors express support for recourse to ADR,[140] which some regard as rapid and inexpensive.[141] Similarly, some replies stress the potential importance of self-regulation in a modern data protection system.[142] Some emphasise, however, that the question of dispute resolution by alternative methods is one that should be dealt with by states, not the Convention.[143] Furthermore, it is a question that ought to be discussed in the European Union context.[144] Perhaps the Convention could confine itself to laying down an obligation to create alternative dispute resolution mechanisms while leaving the substance to domestic legislation.[145]

169. Various contributors observe that if the decision is taken to resort to ADR, this should in any case not limit the other remedies available to the persons concerned.[146] Recourse to ADR could not then be a mandatory stage prior to any judicial remedy - or other remedy still involving public authority, just as it could not be the only means of settling disputes available to the persons concerned.[147] Where ADR was resorted to, it could for example be recommended that existing arbitration bodies be involved in the application of data protection.[148]

170. Several contributors mention the importance of the role which the **data protection authorities** - including data protection officers - can play in settling disputes. For

[136] Opinion of the APEP.

[137] Opinion of the EMOTA.

[138] Opinion of the Cyberspace Law and Policy Centre; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International.

[139] Opinion of the CNIL; opinion of the UK Ministry of Justice.

[140] Opinion of the FEDMA; opinion of the UK Information Commissioner's Office; opinion of the UK Ministry of Justice.

[141] Opinion of the FEDMA.

[142] Opinion of the UK Information Commissioner's Office.

[143] Joint opinion of the AFME and BBA.

[144] Opinion of the CEA.

[145] Opinion of the Direccao-Geral da Politica de Justica.

[146] Opinion of the CIPPIC.

[147] Opinion of the CNIL.

[148] Opinion of the German Insurance Association.

example, some consider that they could be given competence to settle disputes.[149] In this connection they need the freedom to establish procedures, and the Convention could lay down a standard-setting framework for the purpose.[150] For example, it would be appropriate to give data protection authorities the power to act ex officio.[151] They could also have the possibility of intervening freely before the ordinary and administrative courts dealing with current cases.[152]

171. **Other.** On a quite different subject, some contributors stress the usefulness of creating **incentives** to respect for data protection (eg. a gradual easing of the administrative requirements based on the firm's background in simply complying with data protection principles, or even exceeding the normal requirements).[153]

[149] Opinion of the GDD; opinion of the UK Information Commissioner's Office.

[150] Opinion of the UK Information Commissioner's Office.

[151] Opinion of the German Insurance Association.

[152] Opinion of the CNIL.

[153] GSI in Europe.

THE LAW APPLICABLE TO DATA PROTECTION

24. Should a rule determining the law applicable to data processing (in cases where different jurisdictions are involved) be considered?

172. **General**. The problem of the law applicable appears important to many contributors, who repeatedly recommend that the rules be clarified, particularly in the context of cloud computing (an example frequently cited). The problem of applicable law is sometimes regarded as an obstacle for organisations not based in the European Union, and wishing to establish processing operations there; European law would apply without its application being justified by a sufficiently strong link between the individual situation and Union law.[154] However, some contributors reply that they are convinced that the current rules on defining the applicable law are effective.[155]

173. The risk that arises here is a classic of private international law: either there is a risk of absence of protection (no law applicable) or more than one set of rules might be applicable.[156] The replies reveal two convergent trends, both calling for greater harmonisation: more harmonisation of basic concepts and rules is desired, and greater clarity in determining the law applicable. On the latter point, a variety of suggestions is contained in the replies.

174. **Harmonisation of basic rules**. It is clear that the harmonisation of national regulations and interpretation in accordance with the Convention would have a positive effect[157] in so far as the question of the law applicable - as long as it is the law of a Council of Europe member state - would be less important if legal systems were harmonised. Accordingly, some contributors highlight the possibility of integrated harmonisation in the most global framework.[158] Promotion of international cooperation, establishment of guidelines on data protection issues and "rules between states" would help resolve the difficulties currently being encountered.[159] So concept definitions should be clarified, as should their application in the member states.[160]

175. Several contributors point to the potentially universal - or global - nature of the Council of Europe Convention and the desirability of promoting it at international level as a **global standard**.[161] Indeed, the Madrid resolution, which is universally

[154] Joint opinion of the AFMI and BBA.

[155] Opinion of the Data Industry Platform; opinion of the FEDMA.

[156] Opinion of the CNIL.

[157] See, for example, the opinion of TechAmerica Europe.

[158] GSI in Europe.

[159] Opinion of the CEA.

[160] Opinion of the EFAMRO-ESOMAR.

[161] Opinion of the AEDH; opinion of the AFAPDP and the OIF; opinion of the CNIL; opinion of Spyros Tsovilis; opinion of the Direccao-Geral da Politica de Justica.

accepted, could be drawn on in the drafting of certain of Convention 108's principles.[162] These considerations are relevant both to questions of applicability of national law and to cross-border data flows: the two sets of issues are clearly linked.

176. **Rule to determine the law applicable to data protection**. The complex nature of the question of applicable law is mentioned in some of the opinions submitted, particularly in such contexts as that of cloud computing.[163] Some contributors stress that it would be a complicated matter to settle this question in the framework of the Convention, especially in view of the role played by the European Union in this connection:[164] coordination is necessary. Clearly, further thought must be given to the question, but perhaps the complexity of the problem would require a case-by-case approach rather than establishing a general rule.

177. Nevertheless, some contributors think that the question should be dealt with in the Convention[165] - in conjunction with Directive 95/46166 - or in any event that this would be desirable,[167] [168] as affording better legal security. Others believe that the inclusion of such a provision might perhaps constitute an obstacle to possible ratification of Convention 108 by non-member states of the Council of Europe,[169] whereas it should be made an attractive instrument for those states.[170] The protection of data and privacy are highly complex and technical issues about which political debate is still ongoing.[171] Some replies state that the Convention should lay down a general principle, leaving the rest to national regulations and international

[162] Opinion of the CNIL

[163] See, for example, the opinion of the UK Ministry of Justice.

[164] Joint opinion of the AFME and BBA.

[165] Opinion of the Bulgarian Personal Data Protection Commission; opinion of the Cyprus Commissioner for Personal Data Protection; opinion of the Czech Office for Personal Data Protection; opinion of the Lithuanian State Data Protection Inspectorate; opinion of the Data Protection Commissioner of Mauritius; opinion of Mydex (point 24); opinion of the Ukraine Data Protection Authority.

[166] Opinion of the EPA; opinion of the German Insurance Association.

[167] Opinion of the CNIL; opinion of the Cyberspace Law and Policy Centre; opinion of the EBF; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International. The T-PD should also look into the question (opinion of the Direccao-Geral da Politica de Justica).

[168] In the opinion of the Albanian Data Protection Commissioner, it is pointed out that the Convention should provide for a rule enabling the states to lay down specific rules on this.

[169] Opinion of the CNIL.

[170] Opinion of CLSR-IAITL-ILAWS.

[171] US Federal Trade Commission.

cooperation.[172] However, one reply says that it is simply not desirable for the Convention to decide the question of the law applicable to data protection.[173]

178. However that may be, different opinions offer possible approaches to determining the law applicable to data protection.

179. With regard to **jurisdiction criteria**, the replies contain different proposals. For example, with each state guaranteeing equivalent protection - in the context of the European Union, say -, an enterprise active in several of its states would be required to comply with only one set of regulations, that of its principal place of establishment.[174] According to certain contributors, each state's rules should be deemed equivalent.[175] Generally speaking, the replies favour the application of a "country of origin principle".[176]

180. Other differences are proposed as regards jurisdiction criteria. Some contributors suggest that the place of establishment of the data controller of the file be taken as the principal criterion, a secondary criterion being the place to which the data controller of the file specifically directs his activity.[177] The direction of activities criterion would be one to take into account in particular when the controller of the file is situated outside the territory of the European Union.[178] It is sometimes suggested that the law applicable should be that of the country where the bulk of the processing operations takes place or, if that cannot be determined, the law of the country where the controller of the file is situated.[179]

181. By contrast, some contributors go so far as to consider that, where several jurisdictions are involved, "the persons concerned should be entitled to choose the most protective legislation in the event of problems".[180] Alternatively, that the law applicable to data protection should be that of the "victim"[181] (the person concerned).

[172] Ukraine – Ministry of Justice.

[173] Opinion of the Italian Garante per la protezione dei dat personali.

[174] Opinion of the EPA.

[175] Opinion of the APEP.

[176] Opinion of the FEDMA; opinion of TechAmerica Europe.

[177] Opinion of the CNIL.

[178] Opinion of the APEP.

[179] Opinion of the EPA.

[180] Opinion of the AEDH.

[181] Opinion of the Senegal Data Protection Commission.

This rule could possibly be seen as the principle, with exceptions being envisaged.[182]

182. Whatever the criteria ultimately adopted, **considerations to be taken into account** in their definition are mentioned in the replies. For example, if the aim is to reduce the risk of "forum shopping",[183] the "compliance burdens" on enterprises should also be limited.[184] Similarly, simplification of the rules is called for in the case of enterprises belonging to the same international group with cross-border activities,[185] in particular by clarifying responsibilities within such groups.

183. Some replies state that any change to the rules in question should entail improvement in the free movement of personal data.[186] Changes to the rules of private international law must not involve a competitive disadvantage for the internal (European Union) market.[187] Nor should any "extra-jurisdictional reach" be introduced.[188] In order to avoid the last-mentioned problem, it is recommended that account be taken of individuals' desire to use the services of suppliers wholly outside the European Economic Area (EEE-EEA) and foster properly informed decision-making.[189]

184. On a different point, the rules determining the law applicable should not permit persons bringing cases against media enterprises to choose a forum where the protection rules are more stringent than those in the state where such enterprises are established, which would pose a risk to freedom of expression.[190]

185. A Convention provision on applicable law should not hamper the domestic protection afforded to consumers.[191]

186. Account must also be taken of the fact that any change to the rules determining the law applicable has implications not only for "B2C" relations but also for relations

[182] The opinion of the Direccao-Geral da Politica de Justica appears to follow this line, recommending that the law of the person concerned be applied where it refers to "national law". However, it emphasises that exceptions should certainly be provided for, especially in the context of the European Union.

[183] Opinion of the CEA.

[184] Opinion of the CEA; opinion of the EMOTA; opinion of the ENPA-FAEP; FEDMA.

[185] Opinion of the Data Industry Platform; opinion of the GDD.

[186] Joint opinion of the AFME and BBA; opinion of the Data Industry Platform; opinion of the EMOTA; opinion of the FEDMA.

[187] Opinion of the APEP.

[188] Joint opinion of the AFME and BBA.

[189] Joint opinion of the AFME and BBA.

[190] Opinion of the ENPA-FAEP.

[191] Opinion of the CIPPIC.

between enterprises and governmental authorities, including law enforcement authorities.[192]

187. Lastly, although the replies received often deal with the question of the law applicable, some of them mention criteria of competence and the need for them to be pragmatic. If appropriate, a distinction could be drawn between civil jurisdiction and criminal jurisdiction; the T-PD concerned should look into this question.[193]

DATA PROTECTION AUTHORITIES

25. How to guarantee their independence and ensure international cooperation between national authorities?

188. Better cooperation is called for.[194] Some contributors observe that cooperation between data protection authorities should probably be the subject of additional measures written into the Convention[195] (others do not share that view and prefer to leave the problem to domestic law[196]): international mechanisms facilitating cross-border cooperation in the application of data protection rights;[197] mechanisms to be defined, such as a common forum;[198] a minimum of regulation should at all events be stipulated.[199] The aim then would be to clarify and facilitate international cooperation - cooperation conditions, joint action procedures - but not to impose it.[200] Some contributors consider, on the contrary, that cooperation has to be imposed where problems are global.[201]

189. It is also proposed that authorities should be able to carry out joint investigations on the territory of several member states - international complaints, cross-border controls[202] - but without this jeopardising their funding.[203] In this connection it is

[192] Opinion of TechAmerica Europe.

[193] Opinion of the Direccao-Geral da Politica de Justica.

[194] Joint opinion of the AFME and BBA.

[195] Opinion of the AEDH.

[196] Opinion of CLSR-IAITL-ILAWS; opinion of Privacy International; opinion of the Ukraine Ministry of Justice.

[197] Opinion of the EBF.

[198] Opinion of the Italian Garante per la protezione dei dati personali.

[199] Opinion of the Lithuanian State Data Protection Inspectorate.

[200] Opinion of the CNIL.

[201] Opinion of the APEP.

[202] Opinion of the Bulgarian Personal Data Protection Commission; opinion of the CNIL.

[203] Opinion of the Bulgarian Personal Data Protection Commission.

important to clarify the powers of authorities to take action abroad.[204] Others observe that effort should be put into the better recognition between data protection authorities of the measures taken by them - including notifications.[205] One contributor went so far as to propose the creation of a supranational authority.[206]

190. Finally, it was stated that Article 13 § 3. b) of the Convention is an obstacle to international cooperation between authorities because it prevents the transfer of personal data involved in disputed processing despite it being necessary to the settlement of disputes.[207]

191. Concerning the independence of these control authorities, the Portuguese Direccao-Geral da Politica de Justica proposes the following criteria: there must be guarantees that the data protection authority is not subject to instructions or conditions such as to hinder its independent decision-making capacity, that is to say there must be no interference of any kind on the part of a public or private entity; and the necessary resources for its functioning must be covered by the public budget.

26. Should their role and tasks be specified?

192. Yes. The AEDH observes that the additional protocol is not very explicit about the functions and powers of the supervisory authorities. All the examples given in the explanatory report deserve to be codified in the actual text of the protocol. The CLPC suggests that the provision be transferred to the Convention itself.

193. In the view of the ICUK, clarification would be welcome in a landscape where the existing national authorities present a multi-coloured patchwork. Their educational role should in any case be kept. The CNIL considers that these authorities' a posteriori role should be strengthened. The Bulgarian Commission requests that an excessive burden should not be placed on these authorities. The CLPC stresses one function in particular: the obligation of accountability, especially to the public, in respect of obligations to deal with complaints. The Italian Garante believes it would be important to clarify cooperation mechanisms between authorities, perhaps by envisaging specific interaction machinery or joint forums.

194. In addition, in the opinion of the EPA and the APEP, their decisions should be mutually recognised by other states parties; this would be valuable, especially with regard to BCRs. The CIPPIC calls for thought to be given to making the decisions of supervisory authorities binding in law through the common law concept of stare decisis.

[204] Opinion of the CNIL.

[205] Opinion of TechAmerica Europe.

[206] Opinion of the Senegal Data Protection Commission.

[207] Opinion of the UK Information Commissioner's Office.

TRANSBORDER DATA FLOWS

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of "transborder data flows" entirely in the Internet age, where data instantaneously flow across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

29. Should there be different rules for the public and private sectors? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

195. Questions concerning TDFs should be considered in parallel with the problems of the law applicable to data protection. One reply contained a warning: in a networking world, there are limits to the extent to which data flows can or should be controlled.[208]

196. Various contributors emphasise that the current approach to the rules on transborder data flows is not suited to the present technological context;[209] individuals involved in the virtual world have their data sent from one jurisdiction to another with just a few clicks, sometimes to a third state outside the European Union which does not guarantee adequate protection.[210] The present approach does not work effectively, being burdensome to persons acting in benign fashion and ineffective for those acting with more malice.[211] The TDF issue should be tackled more realistically.[212] At the very least, it should be stated in the context of the Internet when such transfers take place;[213] the concept of TDF must be clarified, or even reconsidered.[214] The work of the APEC was mentioned on one occasion when a more workable system was called for.[215]

---

[208] Opinion of CLSR-IAITL-ILAWS.

[209] Joint opinion of the AFME and BBA; Opinion of the Czech Office for Personal Data Protection.

[210] Opinion of TechAmerica Europe.

[211] Opinion of CLSR-IAITL-ILAWS.

[212] Opinion of the UK Information Commissioner's Office.

[213] Opinion of the Albanian Data Protection Commissioner; opinion of the Bulgarian Personal Data Protection Commission.

[214] Opinion of the EBF; opinion of the Italian Garante per la protzeione dei dati personali.

[215] Opinion of the US Federal Trade Commission.

197. Several contributors consider that "the approach in principle should not be changed" and that adequate protection is required.[216] Similarly, regarding the requirement of adequate protection, it is stressed that the provisions of the additional protocol should be incorporated into the Convention,[217] if appropriate by clarifying the rules.[218] By contrast, some replies call for a new legal instrument, separate from the Convention, containing the necessary detailed rules.[219] Others observe that the Convention is general in character and that it is rather the responsibility of the member states to deal with this complex question,[220] whereas national differences aggravate the present practical difficulties.[221]

198. Contributors are interested in the **definition of adequacy**. Some believe that a list of minimum guarantees defining "adequate level of protection" should be drawn up,[222] possibly modelled on what is being done in the European Union.[223] Some argue that Convention 108 should recognise explicitly the decisions on adequacy taken by the European Commission on the basis of Article 26 of Directive 95/46.[224] However, others criticise what is done at the European level, emphasising that what the Commission demands is sometimes more a matter of equivalence that of adequacy;[225] the Convention should reassert that only adequacy is required.[226] Thus the process could be faster and simpler.[227] The Convention could make the assessment process more transparent and, in this context, could be at the heart of developing widely recognised standards.[228]

199. More specifically, it is suggested that adequacy could be assessed on the basis of broad data processing sectors - the financial sector, IT sub-contracting, PNR etc. -

[216] Opinion of the AEDH, in favour of the requirement of an adequate protection standard. See also the opinion of the UK Ministry of Justice.

[217] Opinion of the Cyberspace Law and Policy Centre; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International; opinion of the Direccao-Geral da Politica de Justica.

[218] Opinion of CLSR-IAITL-ILAWS.

[219] Opinion of the Cyprus Data Protection Commissioner.

[220] Opinion of the FEDMA.

[221] Opinion of CLSR-IAITL-ILAWS.

[222] Opinion of the Albanian Data Protection Commissioner; opinion of the Bulgarian Personal Data Protection Commission.

[223] Opinion of the Albanian Data Protection Commissioner.

[224] Opinion of the APEP.

[225] Opinion of CLST-IAITL-ILAWS.

[226] Opinion of the UK Information Commissioner's Office.

[227] Opinion of the UK Information Commissioner's Office.

[228] Opinion of CLSR-IAITL-ILAWS.

;[229] for example, a sector could be deemed to guarantee adequate protection even if the country of establishment does not offer adequate protection guarantees.[230] So adequacy should not mean a general analysis of the law of the third party state concerned, but should rather relate to the particular circumstances of the case, and in particular the controller of the file - or the sub-contractor - located in the third party state, the law of that state being only one factor in the analysis.[231] Some replies also link the adequate protection principle directly to the accountability principle.[232]

200. In the European Union context, when a third party state does not guarantee adequate protection, there are various tools which may nevertheless make TDFs possible. Some contributors call in this connection for better recognition, in the European Union context, of **Binding Corporate Rules [BCR]** or **Model Contractual Clauses [MCC]** so that data transfers inside an international group of companies subject to the same strict rules do not need specific authorisation from the data protection authorities;[233] the rules should be simplified.[234] The authorisation regime poses problems of time taken and costs incurred;[235] formalities should be simplified in cases of recourse to MCCs or BCRs approved by the authorities.[236] Greater flexibility is moreover desired in model contract clauses which, in the European Union at present, for example, do not reflect the reality of cloud computing so that the model becomes inappropriate.[237] It would also be desirable to promote TDF codes of conduct accepted by all authorities for the protection of the relevant data.[238]

201. Some of those who replied consider that **minimum international rules** should be laid down for TDFs.[239] That is the purpose of the Madrid resolution, which should be incorporated into a binding text.[240] But in all hypothetical cases where such minimum

[229] Opinion of the Albanian Data Protection Commissioner.

[230] Opinion of the UK Information Commissioner's Office.

[231] Opinion of the UK Information Commissioner's Office. The US Federal Trade Commission also notes that the situation of the data recipient is not taken into account; opinion of the UK Ministry of Justice, referring to the Madrid Declaration as a starting-point for reflection.

[232] Opinion of TechAmerica Europe; opinion of the UK information Commissioner's office.

[233] Joint opinion of the AFME and BBA.

[234] Opinion of the Data Industry Platform; opinion of the EMOTA.

[235] Opinion of the German Insurance Association.

[236] Opinion of the AFCDP (p.4).

[237] Joint opinion of the AFME and BBA.

[238] Opinion of the CEA.

[239] Opinion of the CEA; opinion of the Cyprus Data Protection Commissioner; opinion of the EPA; opinion of the German Insurance Association; opinion of the AFCDP.

[240] Opinion of the APEP.

rules are desirable, the potential risk of a "race to the bottom" [241] should be borne in mind; some replies observe that such a race would be the inevitable consequence of an attempt to establish global minimum rules, destroying protection of privacy in a cross-border context and thus making that minimum undesirable.[242] Others point out that before thinking about global minimum standards, it is necessary to establish the procedural framework for their definition, involving all regions and all the parties concerned.[243]

202. Finally, on another aspect of the question, the data protection officer (DPO) could play a part with regard to TDFs, and a European DPO might be appointed for a group of companies present in different European Union countries.[244]

[241] Opinion of the CIPPIC.

[242] Opinion of the Cyberspace Law and Policy Centre; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International.

[243] Opinion of the US Federal Trade Commission.

[244] Opinion of the AFCDP.

ROLE OF THE CONSULTATIVE COMMITTEE

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the hitherto primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

203. Most of those who replied to this question are in favour of reinforcing the role of the Consultative Committee, though some think it should remain unchanged.

204. The committee should evolve to become a veritable data protection authority, with responsibility, in its monitoring role, for identifying innovations well in advance and making relevant recommendations and, in its disputes resolution role, for receiving complaints where the parties are faced with a cross-border problem (AEDH). The Mauritius Data Protection Commissioner points out, with regard to disputes, that the national authorities and also individuals should be able to make application to this Committee once it becomes a binding authority. A stronger monitoring role would permit verification of the manner in which the Convention is implemented at national level and provide for action to be taken where it is poorly implemented (CNIL). Its role should be strengthened only in respect of supervisory functions (CEA Insurers of Europe), or these functions but also in the issuing of standards (Cyprus Data Protection Commissioner; CLSR-IAITL-ILAWS consortium), or only in issuing standards (European Privacy Association). The Committee should have a part to play in coordination of practices, experience and suggestions made by national data protection authorities, as well as a monitoring role in respect of international cooperation (Czech Office for Personal Data Protection; Lithuanian State Data Protection Inspectorate).

Role in preparing legislation

205. However, care must be taken to ensure that this does not create additional burdens on the states parties and other national authorities. Any duplication with other existing supra-national bodies, and adoption of contradictory standards, must be avoided (ICUK). The Data Industry Platform believes there there is a real risk of duplication and opposes the idea of adding an extra layer to institutions which already exist. As they see it, standard-setting, dispute resolution and monitoring functions are matters for which self-regulation is the best solution.

206. The Cyprus Data Protection Authority and the Italian Garante both point out that any strengthening of the Committee's role will depend on the human and financial resources made available. The Garante therefore argues that steps should be taken to guarantee the availability of those resources.

207. The CNIL offers a suggestion regarding the membership of the Committee. In view of its "absolutely essential" part in the practical architecture of the Council of Europe, the CNIL considers that it would be highly desirable to review its composition. Since the data protection authorities bear prime responsibility for the application of Convention 108, and because these authorities have the benefit of practical experience and expertise, they should be the ones to appoint representatives to the Committee, not the governments. The government representatives are the only persons present on the European Committee on Legal Cooperation, which is involved in drafting texts.

208. The American FTC suggests that the revision of the Convention be used as an opportunity to think about the contribution and support which the Committee might seek from industry and other key players. The role and the work of the ENISA Permanent Stakeholder Group could be taken as an example of how to obtain backing and facilitate dialogue with industry about the Convention, by reason of the important part which that group plays in the legal framework of data protection in the European Union and elsewhere in the world.

AEDH

CONSULTATION SUR LA MODERNISATION DE LA CONVENTION 108

L'AEDH remercie le Conseil de l'Europe, non seulement pour son initiative de moderniser la Convention 108, mais aussi pour la qualité de ses questionnements au regard des enjeux actuels. En effet les défis actuels sont très globaux, tant par l'insertion des technologies de l'information dans tous les domaines de la vie quotidienne ou dans le cadre d'évènements exceptionnels, que par le rythme des innovations et leur caractère mondial.

L'AEDH voudrait cependant insister en introduction sur son appréciation générale de la Convention. Les principes de base posés par la Convention et son Protocole additionnel sont toujours pertinents mais doivent tous être renforcés ou précisés pour assurer une protection effective. En effet, les pressions économiques pèsent maintenant pour exploiter les données personnelles à des fins d'extension du business à l'insu des personnes ou en leur proposant des avantages qui les conduisent à renoncer individuellement à la protection. De même, les Etats sont tentés d'exploiter le potentiel des technologies de l'information non plus seulement à des fins de meilleure efficacité administrative, mais également à des fins de contrôle des populations d'une manière de plus en plus excessive à la faveur d'une période « sécuritaire ».

Dans un tel contexte, le renforcement des obligations et des droits qui découlent de la Convention sera cependant insuffisant si des mécanismes audacieux de suivi et d'alerte ne sont pas conjointement mis en œuvre.

Enfin, il convient de constater que face à la mondialisation des pratiques et des traitements de données, l'ONU n'ayant pas pris d'initiative pour rendre contraignant les principes directeurs que l'Assemblée Générale a adopté en 1990 pour régir ce domaine, une responsabilité particulière échoie de fait au Conseil de l'Europe pour faire de son instrument, un instrument de réelle portée mondiale. C'est pourquoi l'AEDH remercie également le Conseil de l'Europe pour cette initiative de consultation publique en ligne ouverte à tous sur le plan mondial.

Objet et champ d'application de la Convention, Définitions

Sur l'approche générale et technologiquement neutre de la Convention

En tant que philosophie générale, l'approche de la Convention est juste. D'autant que les principes généraux qu'elle pose répondent tous aux risques présentés par la manipulation de données numérisées (par exemple : principe de finalité légitime versus la facilité de détourner la finalité de données une fois numérisées ; principe du droit d'accès des personnes à leur données versus des données conservées par des tiers peuvent ne pas être pertinentes, à jour ou complètes au regard d'une certaine finalité).

Cependant, l'application effective de la Convention requière pour chaque traitement de données une interprétation des principes de base qu'elle pose. Par exemple, telle finalité est-elle légitime, telle collecte de données est-elle pertinente dans tel contexte ? Et à quelles conditions ?

Par ailleurs l'usage de certaines technologies de l'information ne sont pas neutres du point de vue des libertés et de la vie privée, puisque pouvant être plus ou moins intrusives. Cela conduit à souhaiter des garanties particulières ou renforcées. Par exemple la publicité par courrier postal sur support papier est moins intrusive que la publicité par messagerie électronique, par téléphone sur téléphone fixe ou sur téléphone mobile. Cette gradation dans les risques d'intrusion a conduit des pays membres du Conseil de l'Europe, notamment de l'Union européenne, et des pays tiers, à prévoir une gradation dans la protection : la publicité postale effectuée à l'aide d'un fichier peut n'être soumise qu'à information préalable avec droit d'opposition, tandis que la publicité effectuée à l'aide de moyens électroniques est soumise au consentement préalable et informé de la personne. Il en est de même si l'on songe à la vidéosurveillance ou à la collecte des empreintes digitales d'une personne, dont les domaines d'application et les modalités de légitimité doivent être très précisément encadrés puisque d'emblée par nature ces technologies ne sont pas neutres au regard des libertés et de la dignité des personnes.

Or les interprétations peuvent varier en fonction de l'intérêt des responsables du traitement des fichiers ou des circonstances.

C'est pourquoi, au delà de la réflexion commune sur les moyens nécessaires pour la mise en œuvre des principes (autorité de contrôle indépendante, responsables internes etc.) le suivi de l'application des principes de la convention est essentiel pour maintenir l'objectif de la convention qui est d'assurer une protection effective des personnes ainsi qu'une équivalence de la protection assurée entre les parties. Une telle activité doit aller jusqu'à l'adoption de textes complémentaires, par domaines et technologies, parfois même pour un traitement de données d'enjeu international particulier.

2. **Définir le droit à la protection des données et le droit à la vie privée ?**

Le traitement des données touche aujourd'hui de plus en plus de domaines d'activité humaine au point que l'ensemble des données relatives à une personne traitées dans l'écosystème des traitements de données qui la concerne, sont des expressions/manifestations/représentations tout à la fois de l'identité de la personne, de sa vie privée et de l'exercice de ses droits et libertés (par exemple comme c'est le cas pour l'application stricte du droit à la protection des données vis à vis des moteurs de recherche où c'est le seul moyen de garantir la liberté d'information des personnes et de plus en plus de moyen de garantir leur autonomie). C'est pourquoi plutôt que de définir le droit à la vie privé de manière extensive au regard des acceptions habituelles, il nous apparaît que l'ensemble des principes de base de la Convention et du Protocole additionnel deviennent avec le recours grandissant à la numérisation, un ensemble de moyens de protection de la personne humaine et cela de manière autonome et interdépendante avec les autres libertés et droits fondamentaux.

3. **Sur la Convention comme instrument d'application globale y compris vis à vis des activités de police et de justice**

Cette approche est absolument vitale, y compris en ce qui concerne les critères de dérogation contenus dans l'article 9, dont peuvent être bénéficiaires des activités de police notamment, mais cantonnées aux limites ainsi fixées. Cette approche a fait ses preuves (cf. en particulier l'arrêt Marpper de la CEDH de 2008) et est déjà complétée opportunément par au moins une recommandation d'application sectorielle (dans le secteur de la police) des principes de base qui est également en cours de mise à jour.

La vraie question qui se pose est de savoir si une Partie peut déclarer ne pas appliquer la Convention à certaines activités. Or l'AEDH estime que les coopérations internationales dans les domaines de la police et de la justice devraient conduire à exclure la possibilité pour les parties de ne pas appliquer la Convention à ces secteurs.

4. **Sur l'opportunité d'exclure du champ de la Convention le traitement de données personnelles destinées à des activités exclusivement personnelles et domestiques**

L'AEDH est favorable à cette exclusion mais avec la limite et dans les conditions suivantes :

- ces traitements ne doivent pas donner lieu à transmission de fichiers de données ou d'extrait de fichiers à des tiers ;

- les services offerts aux personnes à des fins de traitements à distance relatifs à ces activités strictement personnelles ou domestiques (telles que de messagerie électronique, de carnet d'adresses, d'agenda, de comptabilité, d'archivage etc..) doivent être soumis à des obligations très strictes d'information de leurs clients sur leurs obligations et d'offre à leur égard de fonctions de confidentialité, et d'interdiction d'exploiter à leurs propres fins des données ainsi traitées.

5. **Sur les définitions du traitement et du maitre du fichier**

La définition du traitement doit absolument inclure la première étape d'une telle opération qui est celle de la collecte des données, et ce, sous quelque forme que ce soit, papier ou numérique.

Dans la définition du maitre du fichier, la notion de fichier devrait être associée à celle des traitements auquel la constitution du fichier donne lieu, car ce sont eux qui manifestent la ou les finalités poursuivies. Par ailleurs, la notion de maitre du fichier/traitement devrait s'appliquer à la personne qui décide non seulement de la finalité du fichier et des traitements mais également de leur mise en œuvre (par exemple en décidant d'avoir recours à un sous traitant). Il est possible que la décision de mette en œuvre un fichier et les opérations de traitement qui lui sont attachées, soit prise par un ensemble de

responsables à des fins collectives et que ces responsables créent une structure pour la mise en œuvre de ces opérations (exemple des systèmes de réservations aériennes commun à plusieurs compagnies aériennes, exemple de fichiers communs à une profession relatif à des clients défaillants etc.). Il apparaît que dans ces cas la responsabilité sur les moyens mis en œuvre revient à cet ensemble de responsables qui doivent donc pouvoir être identifiés.

6. Sur l'ajout de définitions

L'application de l'ensemble des principes de protection des données, selon les traitements en cause, peut relever de différents éléments nécessaires à sa mis en œuvre, et donc relever le cas échéant de plusieurs intervenants de la chaine des acteurs impliqués. Ainsi, en effet, outre la définition du maitre du ficher et des traitements, il est devenu indispensable d'ajouter une définition **du sous-traitant** et de fixer ses obligations, mais également une définition du **fabriquant d'équipements** techniques que ceux-ci soient **matériels ou logiciel.** On pourrait également s'interroger sur la nécessité d'expliciter les obligations d'information et de conseils que certains autres acteurs intervenant dans la diffusion et dans l'installation de certaines applications, notamment nouvelles, devraient avoir alors qu'ils n'ont pas de responsabilité dans la mise en œuvre du traitement lui même. Par exemple si des conditions ont été édictées pour la mise en œuvre de tel logiciel, ou de système de vidéosurveillance, **les distributeurs** de tels équipements devraient eux mêmes informé leurs clients potentiels de ces conditions.

Enfin, l'industrialisation des processus de traitement de l'information dans un contexte concurrentiel et mondial conduit également à ce que bien des aspects de l'application des principes de la protection des données relèvent aussi des **organismes ayant des fonctions de normalisation**. Ceux-ci ont divers statuts publics ou privés, sont de portée nationale, régionale ou surtout internationale, et il convient qu'ils soient également visés dans les textes comme ayant l'obligation de prendre en compte les principes de protection, de rendre transparents leurs projets, d'en saisir les autorités de contrôle lorsque un projet de norme est de portée nationale, et d'en saisir au moins pour avis le comité de la Convention lorsque leur portée est internationale.

Sur les principes

7. Sur la proportionnalité et la minimisation des données

Le principe actuel selon lequel les données doivent être adéquates, pertinentes et non excessives au regard de la finalité est en pratique interprété comme celui de la proportionnalité. S'il y a un doute, alors en effet ce principe doit être réécrit dans le sens de la **nécessité et de la minimisation**. Cependant, il peut arriver que ces principes conduisent encore à une exagération au regard des droits fondamentaux en cause c'est pourquoi le **critère du non excessif au regard des libertés et droits fondamentaux** en cause au regard d'un projet de traitement de donné particulier doit être cumulativement maintenu.

8. Sur le rôle du consentement

La question du consentement ne devrait pas être envisagée en relation avec le principe de transparence et d'information de la personne, mais doit être mis en œuvre dans tous les cas, comme l'un des moyens pour conférer une légitimité à la finalité d'un traitement auquel auront été appliqués par ailleurs tous les autres principes (proportionnalité, sécurité, etc.). En tout état de cause, le consentement ne devrait pas être utilisé comme moyen de faire renoncer la personne concernée à la protection.

9. Sur l'opportunité d'une liste des fondements de licéité d'un traitement

Pour aller dans le sens d'une application plus homogène de la Convention, établir cette liste pourrait être opportun.

10. Sur l'opportunité d'introduire le critère de compatibilité entre la finalité d'origine de la collecte des données et des traitements ultérieure.

Pour l'AEDH, il est clair que tout traitement nouveau effectué à partir de données collectées pour une finalité explicite, ne devrait être possible que sur la base du consentement de la personne concernée et sans perdre les avantages antérieurs liés à la finalité d'origine, ou sur la base d'une législation.

11. Sur l'opportunité de prévoir de nouvelles catégories de données sensibles

Sont citées dans la consultation les données telles que les identifiants nationaux et les données biologiques ou biométriques.

On est en droit de se demander si au nom de la protection de la personne humaine, de telles informations en tant qu'identifiants sûrs d'une personne devraient même exister, surtout quand elles concernent tous les membres d'un peuple et non certaines personnes pour des motifs particuliers au regard d'une nécessité de sécurité publique (nous ne parlons pas ici des informations biologiques nécessaires dans le cadre de prévention ou de traitements médicaux).

L'existence de tels systèmes d'informations est très dangereuse dans toutes circonstances exceptionnelles, telle qu'en cas d'invasion ou de changement de régime devenant non démocratique. De plus, ces systèmes d'attachement physique des personnes à l'Etat rompt le contrat social et repose sur l'idée que tout citoyen est un délinquant potentiel, ce qui n'est pas acceptable.

Il doit donc être prévu pour ces données, non pas une protection renforcée comme pour les autres données « sensibles » destinées à prévenir les risques de discrimination (race, opinions etc), mais une interdiction qui ne peut être levée que sur la base des critères prévus à l'article 9 de la Convention.

12. Sur la protection de certaines catégories de personnes

Les enfants sont cités dans la consultation, mais ils ne sont qu'un exemple de population vulnérable. Il est évident que le fichage de ces populations et les traitements de données les visant peuvent présenter des risques particuliers soit en terme de pressions sur ces personnes, soit en terme au contraire d'exclusion de l'exercice de leurs droits. Il existe cependant des conventions internationales concernant les enfants et d'autres populations vulnérables et notre sentiment est que c'est dans la mise en œuvre de la Convention 108 qu'il convient de tenir compte de la philosophie des protections prévues dans ces différents instruments.

Ainsi la référence à ces textes et à ces philosophies de protection devraient être faites dans des termes généraux et adéquats dans la Convention 108, et des travaux complémentaires devraient être engagés par le Comité consultatif de la Convention sur les modalités d'application de la convention au regard de chacune des populations vulnérables.

13. Sur l'information des personnes concernées en matière de violation du principe de sécurité

Une telle précision serait très utile mais il devrait en même temps être mis à la charge des Etats parties à la Convention l'obligation de prendre des mesures pour prévenir les risques consécutifs à de telles violations pour les personnes concernées, pour établir les réparations et punir les auteurs y compris en cas de négligence.

14. Sur l'opportunité de dispositions concernant les données de trafic de communication et de localisation.

S'agissant de données relatives à la liberté de communication (données de trafic) et d'aller et venir (localisation), il est évident qu'elles ne devraient pas être transmises à des tiers et/ou conservées sous une forme détaillée permettant l'identification directe ou indirecte des personnes concernées par des tiers (les opérateurs et fournisseurs de services), sauf à la demande de la personne concernée ou pour un besoin de facturation dans la mesure où il existe – et dans les circonstances particulières relevant de l'article 9 de la Convention – une investigation sur une personne particulière décidée sous le contrôle d'un juge, pour des motifs de sécurité publique. En ce qui concerne les données de trafic, leur conservation à des fins de facturation se justifie de moins en moins puisqu'on voit se développer des pratiques commerciales au forfait illimté.

Nous pensons qu'il devrait en être de même des requêtes formulées par une personne sur un moteur de recherche. Ces requêtes ne devraient jamais être conservées par le moteur de recherche sous une forme permettant d'identifier directement ou indirectement la personne concernée (liberté d'information) mais par elle même si elle le souhaite et pour ses besoins propres.

15. Sur les mesures destinées à la responsabilisation

Dans la mesure où les principes posés emporteraient l'obligation pour les responsables de fichiers/traitement de les respecter, que les autorités de contrôle ont pour mission de les faire respecter (pouvoir de contrôle et de sanction le cas échéant), et que des sanctions seraient prévues en cas de non application, une telle approche ne serait pas indispensable. Cependant la complexité croissante et l'explosion du nombre des traitements, ainsi que le rythme des innovations technologiques, conduisent à penser qu'au delà d'un certain niveau d'informatisation, les organismes/maitres de fichiers devraient être dans l'obligation de se doter d'une organisation et de mécanismes internes de promotion et de contrôle de l'application des principes.

16. Sur l'approche « privacy by design »

Nos commentaires à propos des définitions prouvent assez qu'en effet, il n'y a pas de protection si l'ensemble des principes posés n'est pas appliqué dès la conception des équipements et des applications. Cette obligation pourrait être simplement précisée dans le texte sans forcément recourir à un vocabulaire marketing tel que celui de « privacy by design ».

Droits - obligations

17. Sur l'ajout du droit d'accès à l'origine des données et à la logique qui sous tend un traitement

Ces deux ajouts sont **absolument nécessaires** compte tenu de la complexité croissante des traitements de données.

18. Sur le lien éventuel entre le droit d'opposition et le droit à l'oubli et sur la possibilité de garantir ce droit et son exercice

La question du droit à l'oubli repose sur de multiples principes de base et tout d'abord celui concernant la durée de conservation des données détenues par un maitre de fichier

(proportionnelle à la finalité) garanti également par le droit de suppression attaché au droit d'accès.

S'agissant de données rendues publiques par la personne concernée sur elle-même, ces données doivent pouvoir être supprimées par la personne concernée en vertu du principe de finalité légitime qui ne regarde qu'elle-même. C'est pourquoi les fournisseurs de services de publication doivent fournir à la personne cliente une fonctionnalité de suivi de la captation de ses informations par des tiers, et une fonctionnalité permettant la suppression.

S'agissant de données rendues publiques sur internet (publication mondiale) par un maitre de fichier (liste de salariés d'une entreprise par exemple), elles ne devraient pouvoir être rendues publiques qu'avec l'accord des personnes concernées. Elles peuvent aussi, selon la finalité et les circonstances, tomber dans le domaine du droit à l'image (pas de publication de photos sans l'accord des personnes concernées) et/ou du droit d'expression et de ses limites au regard du droit à la vie privée. Mais dans ce dernier domaine, même en Europe, il n'y a pas encore de consensus sur les limites, c'est pourquoi, compte tenu des enjeux de la publication sur internet, une initiative visant le rapprochement des points de vue et des procédures – sous le contrôle du juge mais de manière rapide – devrait être prise au sein du Conseil de l'Europe et le cas échéant en relation avec l'UNESCO.

19. Sur l'opportunité d'un droit garantissant la confidentialité et l'intégrité des systèmes d'information

Il nous apparaît que l'article 7 de la Convention prévoit déjà la prise de mesures appropriées contre, notamment, l'accès et la modification des données non autorisées, c'est à dire la prise de mesures de nature à assurer la confidentialité (pas d'accès non autorisé) et l'intégrité des données (pas de modification non autorisée). Pour garantir ces besoins cela conduit en pratique à prévoir des mesures techniques particulières reposant sur le chiffrement (avec beaucoup de précisions sur qualité des algorithmes retenus, la longueur des clefs, les procédures de protection des clés etc). Le principe des sanctions

est prévu à l'article 10 de la Convention. Les précisions techniques nous paraissent relever plus d'une activité de suivi et de recommandations avec évolution dans le temps.

20. Opportunité d'introduire un droit à ne pas être localisé/tracé (identification RFID)

La problématique des systèmes d'information incluant des puces RFID est la même que pour tout autre système de données. Ce qui fait défaut actuellement, ce sont les mesures de mise en œuvre qui doivent être fonction des finalités du traitement des données. Ainsi à la sortie d'un magasin, les puces RFID apposées sur un bien à des fins de gestion des stocks devraient être inhibées systématiquement de manière à ce que la personne qui a acquis le bien ne puisse être suivie. D'autres puce RFID peuvent avoir d'autres finalités, telle que celles inclues dans les passeports électroniques : ici ce qui est en cause ce n'est pas que la puce soit rendue illisible à tout jamais, mais que les données soient chiffrées et de manière à ne pouvoir être lues sans l'accord de la personne qui en est le porteur.

Pour le reste le droit de ne pas être localisé/tracé dépasse le cadre des puces RFID, et concerne aussi les téléphones portables et les applications de géo localisation (cf infra). C'est pourquoi l'AEDH constate que, tant que les technologies ne peuvent par elles-mêmes garantir des libertés fondamentales, c'est par le truchement de l'application appropriée des principes de base du droit à la protection des données qui doivent et sont de nature à en protéger l'exercice : ici en interdisant par exemple la conservation des données.

21. Sur l'opportunité d'un droit à l'anonymat des utilisateurs des technologies de l'information et de communication

La vie sociale repose sur toute une dialectique de l'identification et de l'anonymat qui ne se retrouve pas, en l'état, dans les conceptions qui président actuellement notamment pour l'établissement des communications. Il y a là un « vice de base ». En effet, par exemple, il devrait être possible de consulter les informations rendues publiques sans avoir à transmettre une information relative à sa personne. De même, il devrait être possible d'acquérir un bien numérique tout en rémunérant l'acquisition sans avoir à s'identifier. Or ce type de possibilité n'existe pas en l'état techniquement (identification de l'utilisateur/émetteur par son adresse internet auprès du récepteur), ou socialement (pas de

monnaie électronique équivalente aux pièces et billets de banque). Dans un tel contexte, tout repose sur la durée de conservation des données collectées pour les besoins de la consultation et de l'achat, durée qui devrait être aussi courte que possible. Or le droit à l'anonymat devrait être garanti techniquement et socialement.

22. Sur l'opportunité d'aborder la question du juste équilibre entre protection des données et liberté d'expression

Oui cette question doit être abordée, le cas échéant dans le sens indiqué en réponse à la question 18.

Sanctions et recours

23. Sur la question des recours collectifs

Une telle procédure devient indispensable compte tenu du nombre de personnes qui peuvent être concernées par un défaut de respect des principes et par la complexité parfois de savoir ce qui s'est passé.

Droit applicable

24. Sur l'opportunité de préciser la règle lorsque plusieurs juridictions sont concernées

En matière de production de biens que des industriels souhaitent diffuser sur plusieurs territoires, à des fins d'efficacité, la pratique est de retenir la réglementation la plus contraignante (assurant la meilleure sécurité). Aussi, on se demande pourquoi il n'en serait pas de même en matière de traitements de données à caractère personnel. En tout état de cause les personnes concernées devraient être en droit de se réclamer de la législation la plus protectrice en cas de problème.

Autorité de protection des données

25. Sur la façon de garantir leur indépendance et d'assurer leur coopération

Le protocole additionnel prévoit le principe de l'autorité de contrôle de la protection des données agissant de manière indépendante. Or son indépendance est essentielle pour donner confiance aux personnes dont les données sont traitées.

L'indépendance peut être assurée selon un faisceau de mesures tenant à :

- son mode de désignation et de composition qui doit garantir son indépendance vis à vis tant du pouvoir économique (règles d'incompatibilités), que du pouvoir politique (si l'organe est collégial et que des parlementaires en font partie, les partis tant au pouvoir que d'opposition doivent être représentés, un représentant de l'exécutif ne peut être membre de l'autorité et si elle n'est pas collégiale une majorité très large (3/5 ?) du parlement doit donner son accord),

- la durée fixe de son mandat et l'impossibilité de radiation de son (ses) membre(s) en raison des missions de l'autorité,

- son mode de financement qui doit être suffisant pour assurer ses tâches, y compris en matière de coopération transfrontalière (taxe sur les dépenses TICs du pays ?), et son mode de contrôle de ses dépenses (non pas a priori par l'exécutif, mais a posteriori par l'organe de contrôle suprême des dépenses des organismes publics),

- son obligation de publier un rapport régulièrement de synthèse de ses activités tant en volume qu'en contenu (mesure contribuant à démontrer son indépendance).

La coopération entre autorités de protection des données devrait sans doute faire l'objet de mesures complémentaires inscrites dans la Convention favorisation d'une part son organisation à bonne fin ainsi qu'à la levée d'obstacles juridiques éventuels à la transmission entre elles de données à caractère personnel qui serait nécessaire au règlement des litiges transfrontaliers.

26. Sur l'opportunité de spécifier leur rôle et leur mission

Le protocole additionnel qui prévoit le principe de l'autorité de contrôle est peu explicite sur ses missions et pouvoirs. Le rapport explicatif donne un certain nombre d'exemples qui mériteraient d'être tous retenus et codifiés dans le texte même : informations de personnes sur leurs droits et obligations, conseil en matière de réglementation et de projets de loi, conseil auprès des maitres de fichiers et autres intervenants, contrôle a priori dans les domaines les plus sensibles, instruction des plaintes, pouvoir de contrôle sur place de sa propre initiative, pouvoir de médiation et d'injonction en cas de déficience, ainsi que de sanction, mission de suivi des innovations et d'alerte des pouvoirs publics lorsque des mesures supplémentaires sont nécessaires, obligation de coopérer avec ses homologues en matière de plaintes et de contrôles transfrontaliers.

Bien évidemment toutes les activités de type normatives devraient faire l'objet de consultation des parties prenantes, en particulier des représentants des personnes concernées et des associations de défense des droits de l'Homme. Cette approche méthodologique devrait être explicite dans le texte de la Convention modernisée.

Flux transfrontières des données

27 à 29.

L'approche de principe en matière de transferts de données (protection adéquate) ne devrait pas être modifiée. La recherche de solutions programmatiques telle que celles reposant sur les règles internes des entreprises qui seraient contraignantes, telles que visée dans la consultation, devrait être encouragée dans les domaines de traitement de données non sensibles.

Par contre nous ne comprenons pas que l'on songe encore à définir un ensemble de principes minimum à promouvoir sur le plan international. Ceux-ci existent déjà et ont été adoptés en 1990 par l'Assemblée Générale de l'ONU sous la forme de principes directeurs, qui d'ailleurs vont jusqu'à prévoir une protection renforcée pour les données sensibles (de même nature que celle de la Convention 108) et même le principe de l'autorité indépendante.

Dès lors il ne paraît pas y avoir d'autre choix responsable à notre avis, étant donné le silence actuel de l'ONU, que celui pour le Conseil de l'Europe d'engager une véritable politique de promotion de sa convention modernisée.

Comité de la Convention

30. Sur l'opportunité de développer ses fonctions : normative, règlement des litiges, suivi

Compte tenu de l'explosion du nombre de traitement des données, du rythme des innovations et du caractère de plus en plus international des pratiques gouvernementales et privées, on ne peut que souhaiter le renforcement du rôle du Comité consultatif de la Convention en une véritable autorité de protection des données, chargée en matière de suivi, d'identifier très en amont les innovations, et de les accompagner de recommandations, et en matière de litige, de pouvoir être saisie lorsque des parties prenantes estiment que des problèmes transfrontaliers se posent.

AFAPDP

Consultation sur la modernisation de la Convention 108 – mars 2011

Contribution des autorités membres de l'Association Francophone des Autorités de Protection des Données Personnelles, avec le soutien de l'Organisation Internationale de la Francophonie

Ce document reprend l'essentiel des contributions des autorités membres de l'**Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)** et le point de vue de l'**Organisation Internationale de la Francophonie (OIF)** sur la modernisation de la Convention 108.
Il est inspiré des contributions de quatre autorités francophones membres de l'association : la Commission nationale de l'informatique et des libertés (CNIL) en France, le Commissariat à la protection des données de l'Île Maurice, la Commission à la protection des données (CPD) du Sénégal et la Commission pour la protection des données de Bulgarie.
L'AFAPDP est membre observateur du comité consultatif de la Convention 108 depuis août 2008.

Synthèse des contributions des autorités membres de l'AFAPDP et de l'OIF sur la modernisation de la Convention 108

Contribuer à la consultation sur la modernisation de la convention 108 et participer à l'effort commun vers l'harmonisation des principes de la législation sur la protection des données personnelles font pleinement partie des missions de l'AFAPDP. En s'associant à la réponse de cette dernière, l'Organisation Internationale de la francophonie (OIF) apporte son soutien aux efforts de l'association dans la diffusion du droit à la protection des données personnelles dans l'espace francophone et témoigne aussi, conformément aux engagements de ses Etats et gouvernements membres, de sa mobilisation en faveur de l'adoption d'un instrument juridique international. Cette modernisation doit permettre à la fois de :

- compléter certaines notions et principes juridiques ;
- harmoniser les législations aux fins d'une meilleure garantie du droit à la protection des données personnelles et de la vie privée ;
- inciter les Etats non dotés à adopter une législation.

Aussi, nos principales remarques concernent l'approche universelle de la convention (1) et certains droits ou principes à approfondir (2).

1. L'approche universelle développée par la Convention 108

A travers les présentes contributions, l'AFAPDP et l'OIF souhaitent recommander :

- l'affirmation des principes de base universellement reconnus, qui donnent un potentiel universel à la Convention et prennent en compte la diversité des cultures juridiques ;
- le maintien d'une approche technologiquement neutre, qui garantit que les droits et obligations des différentes parties demeureront valables indépendamment de l'évolution des technologies ;
- le maintien de l'équilibre entre liberté de circulation de l'information et respect de la vie privée qui défend l'idée selon laquelle les responsables de fichier doivent s'assurer que les avantages qu'ils peuvent obtenir du traitement automatisé des données n'aboutissent, en même temps, à fragiliser la position des personnes concernées[1] ;
- la sensibilisation accrue à la ratification par des Etats non membres du Conseil de l'Europe, réitérée par ailleurs en novembre 2010 lors de la 30e conférence du Conseil de l'Europe des ministres de la justice ; de même, la démarche de consultation, que le comité consultatif du

[1] Extrait du rapport explicatif de la Convention 108.

Secrétariat général de l'Association francophone des autorités de protection des données personnelles
Contacts : 8 rue Vivienne – CS 30223 – 75083 PARIS Cedex 02
Téléphone : +33 (0)1 53 73 25 96 / Fax : +33 (0)1 53 73 22 56 / Courriel : afapdp@cnil.fr

Conseil de l'Europe a souhaité « aussi large que possible », nous parait particulièrement souhaitable.

2. *La mise à jour de certains articles de la Convention 108*

Sur la base des contributions reçues par le secrétariat de l'AFAPDP et qui sont transmises au Conseil de l'Europe, nous souhaitons souligner l'importance de :

- mettre à jour la Convention 108 suite à l'apparition de technologies modernes et parfois menaçantes vis-à-vis du respect de la vie privée et de la protection des données. Face aux techniques nouvelles de localisation, reconnaissance biométrique… ;
- multiplier les garanties en matière de protection des données personnelles et assurer une complémentarité de ces garanties ;
- définir précisément les principes et principales notions, ainsi que les responsabilités des différents protagonistes dans l'utilisation des fichiers automatisés de données personnelles ;
- accorder une attention aux populations particulièrement menacées, notamment les jeunes, en valorisant le rôle de sensibilisation des autorités de protection.

AFCDP

Paris, le 23 avril 2011

Contribution de l'AFCDP à la Consultation du Conseil de l'Europe sur la modernisation de la Convention 108, « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »

Le Délégué à la protection des données : l'acteur essentiel du nouveau dispositif global de la protection des données personnelles.

Etant donné que le «Data Protection Officer » (DPO) ou Correspondant Informatique et Libertés est devenu un acteur incontournable de la nouvelle approche de la protection des données personnelles, ce qui n'était pas le cas en 1981, l'AFCDP considère qu'il est important que les lois des Etats parties à la Convention 108 réservent toutes une place à la fonction de DPO, ne serait-ce que facultative mais à tout le moins incitative.

L'AFCDP

L'AFCDP (Association Française des Correspondants à la Protection des Données Personnelles) a été fondée en 2004 après la création de la fonction de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour **Correspondant Informatique et Libertés**). Le CIL est la transposition en droit français « détaché à la protection des données à caractère personnel » prévu par la Directive 95/46/EC.

L'AFCDP est, pour la France, l'association représentative de cette profession émergente : plus de la moitié des entités ayant désigné auprès de la CNIL un Correspondant Informatique et Libertés y adhère. Elle a pour objectif de :

- promouvoir la fonction de Correspondant et d'en faire un métier,
- proposer un cadre d'échanges en développant un réseau en France et à l'international,
- identifier les bonnes pratiques utiles aux Correspondants,
- représenter la fonction, en ayant la primeur de l'information, en agissant pour faire valoir la position de ces professionnels.

La richesse de l'AFCDP réside dans la diversité des profils des adhérents : CIL, juristes et avocats, responsables RH, informaticiens, professionnels du marketing et du e-commerce, déontologues, Risk Manager, universitaires et étudiants, archivistes, experts en sécurité, qualiticiens …

Les travaux de l'association s'appuient sur une quinzaine de groupes de réflexion sur des sujets tels que : Durée de conservation, Géolocalisation et Libertés, Données de santé, Données Clients et Prospects, Rôle et Missions du Correspondant Informatique et Libertés, Flux transfrontières, Notification des violations de traitements de données personnelles, Référentiels et labels, Réutilisation des données publiques, Conformité des réseaux sociaux, etc.

S'appuyant sur sa connaissance concrète de la fonction de CIL et des pratiques des organisations en matière de protection des données personnelles, l'AFCDP souhaite apporter sa contribution à la modernisation de la Convention 108, suite à l'appel lancé par le Conseil de l'Europe[1].

Elle souhaite faire également un retour sur l'expérience acquise depuis 2004 par les DPO français pour éclairer le débat.

Le « DPO » en France

Le « DPO[2] » à la française a été introduit dans nos textes par la loi du 6 août 2004 modifiant la première loi de protection des données personnelles en France, la loi du 6 janvier 1978, dite « Loi Informatique et Libertés ». Il y est désigné comme le Correspondant à la protection des données personnelles qui est plus couramment

---

[1] *« Modernisation de la Convention 108 : Votre avis nous intéresse ! http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_FR.pdf*

2 « Data Protection Officer »

dénommé CIL (pour Correspondant Informatique et Libertés). Sa mission est « *d'assurer, d'une manière indépendante, le respect des obligations prévues par la présente loi* ». Il ne se substitue pas au responsable de traitement qui reste responsable de la conformité du traitement aux exigences légales.

Sa désignation est actuellement laissée à la discrétion des responsables de traitement qui bénéficient toutefois de deux incitations :

- une incitation d'origine législative : ils sont exonérés de formalités de déclaration à la CNIL, sauf lorsque le traitement est assorti d'un flux hors de l'Union Européenne[3] ;
- une incitation à l'initiative de la CNIL, qui a créé un service et des outils spéciaux pour les Correspondants afin de leur apporter une aide spécifique dans l'exercice de leur mission.

Depuis cinq ans le nombre de CIL a très fortement cru : prêt de 8.000 organismes ont nommé un CIL, certains partageant leur correspondant, plus de 2.000 individus exercent cette fonction en France : chaque Français a aujourd'hui une partie de ses données personnelles traitée par un organisme qui agi sous la vigilance d'un CIL.

Depuis sa création en 2004, l'AFCDP a été témoin d'une réelle évolution des mentalités à la fois au sein des responsables de traitement et des « chargés » de la protection des données. Les premières interrogations levées, l'association a pu constater que **le CIL est aujourd'hui la référence en matière de bonne protection des données à caractère personnel**.

L'utilité du DPO est affirmée; tant pour les personnes concernées, qui trouvent en lui un interlocuteur, intermédiaire auprès du responsable de traitement, que pour le responsable de traitement qui bénéficie ainsi d'un avis expert sur la mise en œuvre des systèmes d'information de plus en plus nombreux et sophistiqués.

Le nombre de professionnels du domaine, en interne comme en externe, ne cesse de croître, au point que l'on assiste à l'émergence d'une véritable profession, ce dont l'AFCDP se félicite.

Contribution de l'AFCDP

L'AFCDP a choisi de se focaliser sur les questions soulevées dans l'appel à proposition, pour lesquelles le CIL (ou le DPO) a un rôle indubitable à jouer.

Plusieurs des questions soulevées par le Conseil de l'Europe vont dans le sens des besoins perçus par l'association, et en particulier de la volonté d'assurer une mise en œuvre concrète des règles par les Responsables de traitement.

L'AFCDP est convaincue que cet objectif ne peut être atteint que si les textes s'appuient sur le DPO.

En effet, si la protection des données doit être l'affaire de tous, l'expérience montre que la matière n'est pas d'abord facile. La règle juridique n'est pas toujours aisément transposable en pratique, que ce soit au niveau technique comme organisationnel. Le DPO joue ainsi un rôle essentiel auprès du responsable de traitement avant la mise en œuvre de tout traitement afin de veiller à sa conformité de bout en bout aux règles de protection des données (appréciation du respect du principe de légitimité et proportionnalité, mentions d'information, fonctionnalités pour l'exercice des droits, mesures de sécurité etc.). Le DPO est aussi présent auprès des préposés du responsable de traitement pour les sensibiliser aux règles qu'ils doivent respecter.

Voici, d'après l'AFCDP, les objectifs qui seraient mieux servis en présence d'un DPO s'ils étaient introduits dans la Convention 108 révisée :

- **L'analyse du traitement envisagé et de ses conséquences**

  En France, le CIL intervient en amont de tout projet de traitement de données à caractère personnel, phase durant laquelle il en analyse toutes les caractéristiques.

  Il est ainsi amené à s'interroger et à porter conseil auprès du responsable de traitement sur :

[3] Ce qui est regretté.

- La finalité poursuivie par le traitement et son caractère légitime : le CIL identifie et documente les textes éventuels qui légitiment le projet (question n°9) ;

- La nature proprement dite du traitement projeté. (question n°5) ;

- Le rôle des parties impliquées, comme le responsable de traitement/maître du fichier et les sous-traitants (questions n°5 et n°6). Sur ce point spécifique, un groupe de travail AFCDP a produit un livrable joint en annexe[4]. L'hypothèse d'introduire une notion de « co-responsabilité » sur un même traitement, semblant difficilement applicable dans le droit français, notre association a porté ses efforts sur la formalisation d'une démarche qui permet d'identifier les différents acteurs impliqués et leurs responsabilités propres. Cette réflexion spécifique serait facilitée si ces acteurs disposaient chacun d'un DPO. Le CIL conseille à son responsable de traitement de veiller à ce que les contrats établis avec les sous-traitants portent les mentions requises par la réglementation sur la protection des données à caractère personnel.

- La proportionnalité de la démarche entreprise par le maître du fichier (question n°7);

- La nécessité (ou non) de collecter chaque donnée personnelle envisagée (principe de minimalisation évoquée à la question n°7);

- La nature et la sensibilité des données personnelles dont le traitement est envisagé (question n°11). Ce critère est pris en compte par le DPO/CIL dans le cadre de son analyse de risques. Sur ce point il nous semble préférable de ne pas introduire de spécifications pour laisser le CIL apprécier chaque situation, chaque contexte. De plus le DPO revoit périodiquement son analyse de risques et peut adapter le niveau de protection à toute évolution (d'usage, technologique, etc.) ;

- Les personnes concernées. Il appartient au DPO, dans le cadre de son analyse de risques, de conseiller à son responsable de traitement toute précaution spécifique adéquate en présence de population pouvant demander une approche particulière, telle que les enfants (question n°12). Sur ce point il nous semble préférable de ne pas introduire de spécifications pour laisser le CIL apprécier chaque situation ;

- L'information de ces personnes (question n°8). Quels que soient les efforts de transparence du responsable de traitement pour communiquer, les personnes concernées peuvent avoir du mal à comprendre certaines mentions d'information qui recouvrent des réalités complexes (publicité comportementale, utilisation de technologies émergentes, partage d'informations avec des tiers); dans ces cas, le DPO paraît être l'interlocuteur privilégié pour apporter une réponse à leurs interrogations ;

- Le type de consentement qui devra être obtenu auprès des personnes concernées (question n°8). Soucieux du principe de transparence, le CIL conseille son responsable de traitement sur la démarche adéquate, en fonction du contexte ;

- Le niveau de protection à apporter au traitement envisagé. L'AFCDP est favorable dans le principe général d'une notification des violations à la sécurité des données (question n°13) sous réserve de modalités d'application réalistes qui accorderaient un rôle pivot au Correspondant Informatique et Libertés. Afin d'éviter un engorgement au niveau des autorités de protection des données, d'éviter des émois inutiles et d'épauler le responsable de traitement, sans pour autant substituer à lui, le DPO peut utilement jouer un rôle de filtre des violations nécessitant une notification à l'Autorité d'une part, aux personnes concernées d'autre part, ou éventuellement un classement avec un ajustement des mesures de sécurité. En toute hypothèse, les incidents seraient tous documentés au bilan du CIL, document destiné au responsable de traitement et tenu à disposition de l'autorité de contrôle ;

[4] Co-traitements : Mais qui est responsable ? – Janvier 2011

- L'organisation de la gestion du droit d'accès (question n°17). Il est plus simple et efficace que les demandes d'exercice des droits d'accès, de rectification ou d'opposition soient centralisées auprès d'un DPO afin qu'elles ne soient pas égarées et qu'elles soient traitées uniformément. L'organisation de la gestion du droit d'accès est de la responsabilité du CIL, dont il surveille la bonne application. Soucieux du droit des personnes, il veille à ce que les informations communiquées à la personne qui en fait la demande la satisfassent, dans la limite des intérêts du responsable de traitement. Quand l'origine de la collecte est disponible, l'information est généralement communiquée. C'est également le cas concernant la logique qui sous-tend le traitement). Sur le sujet spécifique du droit d'accès, l'AFCDP a créé un Index[5] qu'elle publie annuellement à chaque date anniversaire de la Convention 108. L'organisation de l'exercice des droits existants pèche manifestement. Pour l'AFCDP, la désignation d'un Correspondant Informatique et Libertés doit s'imposer afin d'assurer l'effectivité de ce droit crucial, qui conditionne l'effectivité des droits de suite ;

- L'organisation de la purge des données et du respect des durées de conservation auxquelles s'est engagé le responsable de traitement ;

- L'organisation des droits de suite, dont celui d'opposition pour motif légitime[6] ou dans le cas de publicité par voie électronique (question n°18).

- L'existence d'un flux transfrontière. Dans ce cas, le CIL en spécifie la raison, le caractérise et recommande à son responsable de traitement les précautions et le formalisme à respecter. L'AFCDP espère naturellement une homogénéisation des règles minimales (question n°28). Un allègement de formalités, y compris en cas de transfert hors UE[7], accompagné d'un certain nombre d'autres mesures incitatives pourraient engendrer la nomination d'un nombre significatif de DPO, ce qui éviterait le risque d'une obligation de désignation qui pourrait être impopulaire. L'AFCDP aspire également à la reconnaissance d'un « DPO européen » qui pourrait officier pour un groupe de sociétés présent dans différents pays de l'Union Européenne et le faire bénéficier des avantages liés à la fonction de DPO dans chacun de ces pays par réciprocité. Une telle mesure est à rapprocher de la question n°25 concernant la coopération entre les autorités nationales. Notre association ne perçoit pas le besoin d'introduire une différentiation de traitement entre secteur public et secteur privé en ce domaine.

Une fois le traitement opéré, le CIL réalise des audits réguliers et est éventuellement amené à émettre des conseils réactualisés auprès du maître du fichier. Il veille notamment à éviter les détournements de finalités (question n°10) et recommande les actions nécessaires si des ajouts ou des modifications étaient apportées aux buts initialement poursuivis.

Pour mener à bien sa mission, le CIL doit procéder à une analyse des conséquences du projet sur la vie privée et les libertés individuelles des personnes concernées. C'est à partir de cette analyse qu'il va indiquer au maître de fichier/responsable de traitements si le projet nécessite l'intégration de certaines fonctionnalités au stade même de la conception. Le DPO joue donc un rôle clé dans le processus de respect de la vie privée dès la conception évoqué dans la question 16.

Dans le cadre de sa veille le CIL se tient informé de toute innovation d'usage (exemple : Réseaux sociaux) et technologique. Il adapte en permanence ses analyses et ses recommandations en conséquence, quelque soient la présence de dispositifs spécifique (questions n°1 et n°14), les éventuels risques spécifiquement induits seraient pris en compte naturellement par le CIL dans le cadre de son analyse de risques.

---

[5] Index AFCDP du Droit d'accès. http://www.afcdp.net/-Index-du-Droit-d-acces-

[6] Concernant un éventuel futur « droit à l'oubli », l'AFCDP a participé aux travaux menées courant 2009 et 2010 sous l'égide de la Secrétaire d'Etat chargée de l'économie numérique.

[7] Lorsque les données sont protégées par les Clauses Standards de la Commission Européenne ou des BCR approuvées par les Autorités compétentes.

- **La responsabilisation du maître du fichier**

  Le DPO, de par sa proximité avec l'organisation et le métier du responsable de traitement, doit être au cœur des initiatives relatives à la responsabilisation du maître du fichier.

  Cette prise de conscience est obtenue par plusieurs moyens parties intégrantes des missions d'un CIL :
  - La sensibilisation : le CIL diffuse au sein de l'organisme qui l'a désigné la « culture » Informatique et Libertés et créé les réflexes propices à une bonne protection des données personnelles et du respect de la vie privée des personnes concernées ;
  - La présentation du bilan : les textes français précisent que le CIL doit établir un bilan annuel qu'il présente au responsable de traitement. Ce document est tenu à la disposition de l'autorité de contrôle. Cette spécificité française nous paraît une mesure concrète répondant à l'objectif de « responsabilisation » du responsable de traitement ;
  - Analyses de valeur, de risques et d'impact : les textes laissent au maître de fichier/responsable de traitement le soin d'adapter le niveau de protection en fonction de la sensibilité et de la criticité du traitement. Ces analyses, menées en amont de tout projet suivant le principe du respect de la vie privée de la conception, sous l'égide du CIL, peuvent être documentées et portées dans le bilan annuel pour les traitements jugés les plus sensibles ;
  - Chartes, procédures, codes de conduite, Binding Corporate Rules, etc. Le CIL peut être à l'origine de la conception et la formalisation de tout document impliquant une prise de conscience par le responsable de traitement et les directions opérationnelles des enjeux liés à la nécessaire protection des données personnelles et de la vie privée.

  De plus, dans l'hypothèse d'une obligation de notification des violations à la sécurité des données (question n°13) l'AFCDP prône une application dans laquelle le Correspondant Informatique et Libertés conseillerait le maître de fichier/responsable de traitement sur la nécessité d'informer la Commission nationale de l'informatique et des libertés ainsi que les personnes concernées, en fonction de l'analyse d'impact qu'il aura menée, naturellement après que le responsable de traitement a pris immédiatement les mesures nécessaires pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données. Cette analyse, au cas par cas, renforcerait la prise de conscience du maître de fichier de ses responsabilités, de l'intérêt des démarches proactives (application du principe du respect de la vie privée de la conception) et de celui d'apporter son plein soutien à son DPO.

  Ces différents points répondent à la question n°15.

  Pour toutes ces raisons, les futurs textes devraient faire du DPO un acteur incontournable de la nouvelle approche de la protection des données personnelles. Il s'agit à notre sens de la mesure phare d'une responsabilisation accrue des maîtres de fichier.

  Par conséquent, il nous paraît important pour la protection des données que les lois des Etats parties à la Convention 108 réservent toutes une place à la fonction de DPO, ne serait-ce que facultative mais à tout le moins incitative.

L'AFCDP reste à la disposition du Conseil de l'Europe pour contribuer aux réflexions qu'elle souhaiterait mener sur la modernisation de la Convention 108 et la fonction de DPO. L'AFCDP se tient également prête à exposer de vive voix les points et arguments développés dans ce document.

* *

Annexes :

- *L'AFCDP se présente – Avril 2011*
- *Tableaux comparatifs des délégués à la protection des données personnelles en Europe – Juin 2009 (3 documents)*
- *Co-traitements : Mais qui est responsable ? – Janvier 2011*
- *Index AFCDP 2011 du Droit d'accès – Janvier 2011*

afme/bba

The voice of banking & financial services

SENT VIA E-MAIL:
data.protection@coe.int

11 March 2011

Dear Sir / Madam,

Joint AFME & BBA response to Consultation on the Modernisation of Convention 108 of the Council of Europe (Automatic Processing of Personal Data)

The BBA (British Bankers' Association) is the leading association for the UK banking and financial services sector, speaking for 216 banking members from 50 countries on the full range of UK or international banking issues and engaging with 42 associated professional firms. Collectively providing the full range of services, our member banks make up the world's largest international banking centre, operating some 150 million accounts and contributing £50 billion annually to UK economic growth.

AFME (The Association for Financial Markets in Europe) represents a broad array of European and global participants in the wholesale financial markets, and its members comprise all pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. AFME participates in a global alliance with the Securities Industry and Financial Markets Association through GFMA (Global Financial Markets Association) to communicate the industry standpoint on issues affecting the international, European and UK capital markets.

Our members welcome the opportunity to comment on the 'Modernisation of Convention 108' and responses to the specific questions that have relevance to the financial services sector are detailed below (some of which is incorporated into our response to the Communication on the Data protection Directive).

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

We agree with the comments made in the Council of Europe position paper distributed at the 32nd International Conference of Data Protection and Privacy Commissioners[1] that "while being drafted in a simple and technologically-neutral way, the fundamental legal standards contained in Convention 108 remain valid". The paper also reminds that Convention 108 was drafted with the clear intention to associate non-European states and is the only existing international legally binding instrument which has the potential to be applied worldwide. Our members feel that if this remains the aim of

[1] 32nd International Conference of Data Protection and Privacy Commissioners[1], 27 – 29 October 2010, Jerusalem, Israel.

Convention 108, then it must not move towards a prescriptive and technology prescriptive format that will deter non European states from ratifying. Indeed, this appears to us to be an ideal opportunity for the Council of Europe to work with The Madrid Resolution Promotion Group and other interested parties to find a palatable and pragmatic global solution.

2. Should Convention 108 give a definition of the right to data protection and privacy?

We think the remit of Convention 108 should be restricted to protecting the right of privacy with respect to the processing of personal data.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes, our members believe that it should.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

We believe incorporating this as an exception will add very useful clarity and allow consistency with Directive 95/46/EC.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list? The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

With respect to 'automatic processing', members would not have any objection to the definition being changed to 'processing' and the definition being in line with that of Directive 95/46/EC rather than 'collection' being subject to a special provision.

With respect to data controllers, it has long been established that there can be more than one data controller in respect of a particular processing activity. However, we do not think the definition of 'controller of the file' in Convention 108 needs to be more explicit on this point. Consideration should be given to the changes in the way data is collected, used and processed in the age of the internet and cloud computing, to ensure that the terminology is not confined by concepts of 'file' or other technology specific mechanisms which may compromise the neutrality and hence broad applicability of Convention 108.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Whilst we can understand the purpose of including a definition of personal data processor which is already included in implementing legislation, our members have difficulty in understanding what the benefit of including a definition of 'manufacturer of technical equipment' would be.

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Members understand the need to retain as little personal data as possible in proportion to the processing purpose, and feel these requirements are already well established in Article 5 of Convention 108. It is important not to set rules that are overly prescriptive in this area because they may conflict with the operating requirements or legal/regulatory obligations financial organisations are subject to and which facilitate the operational efficiency of their business. Financial organisations are therefore best placed to determine what personal data they need to keep and for how long in light of their legal and regulatory obligations. It is difficult to see what additional value an additional principle of data proportionality or minimalisation would provide for the individuals the Convention is aimed at protecting.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Convention 108 does not currently incorporate specific processing conditions that data controllers should meet. Members do not feel that Convention 108 should introduce conditions necessary to make the processing lawful and most particularly not any one condition currently seen in implementing legislation in isolation. The discretion of data controllers to determine when consent is the most appropriate condition to rely on to legitimise processing must not be diminished in any way. Consent is often not appropriate in the circumstances (as has been noted previously on more than one occasion by the Article 29 Working Party) and data controllers must be allowed to rely on the most appropriate processing condition to the circumstances. Consent needs to be appropriate and pragmatic in order to be credible and effective.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

Please see our answer in response to question 8 above.

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Article 5 b. requires that personal data not be used in any way incompatible to the purposes for which the personal data are collected and we believe this already adequately addresses this point.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

Members consider it important to recognise that very often it is the context in which personal data is processed which determines the degree of risk and/or harm to individuals and so personal data which is not categorised as 'sensitive' can be of great sensitivity in certain circumstances.

In addition, there are circumstances where a data controller will have legitimate grounds for processing sensitive personal data even though the individual concerned may not be happy with this or where the individual may not be specifically aware that sensitive personal data is processed in situations where it is to their benefit and does not in any way prejudice their rights or freedoms.

For the above reasons we believe it unnecessary to have a 'sensitive personal data' category defined in Convention 108.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

The protection of children is not an issue of specific relevance to the financial services industry.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Members do not think that Convention 108 should introduce a specific right for individuals to be informed of data security breaches. We feel this would be an overly prescriptive measure and would add no additional protection to individuals or prevent breaches from occurring.

Financial institutions fully understand there are circumstances that require notification to financial and/or data protection regulators and affected individuals in the event of a breach. Many financial services regulators already require financial organisations to report specific types of breaches and it is important not to be operating in a dual regime which could either provide for duplicative or conflicting obligations.

It is also important to look at the lessons learned in other countries where an overly prescriptive breach notification regime has failed to meet its objectives, and has instead created confusion and unnecessary alarm to individuals, or where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Members do not believe it necessary to introduce special rules in this area.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Members do not believe it is necessary to introduce this into Convention 108.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Members believe this requirement is already implied by the principles and aspirations of Convention 108 negating the need for a specific principle to be introduced. However, if it is to be introduced it must be high level principle and not prescriptive as to measures that should be taken.

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

Implementing legislation already addresses both of these points. Members have no objection in principle to the introduction of these rights as long as they are at a high level and do not go beyond the current requirements of Directive 95/46/EC (i.e. the obligation is to disclose the source of the personal data *if known*, there is no obligation to keep details of the personal data sources).

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

The right of opposition should be a qualified right on the basis of legitimate grounds as it is not always appropriate to process personal data on the grounds of consent.

The 'right to oblivion' is one of the most difficult topics under current consideration and perhaps the one most affected by advances in technology, an issue which has particularly come to the fore with the use of social networks. It is a key area where social norms are not yet established and where practical application will be extremely difficult and not always appropriate.

The right to be forgotten cannot be absolute in all circumstances. There are many legitimate, including legal, reasons why a financial organisation should justifiably be able to keep records of its interaction with the individuals it interacts with, even if they might prefer those records to be deleted. For example, continuity of business, management information and records, employee references and historical records.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

We believe this is already taken as a given obligation under Article 7.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

We believe this should not be introduced into Convention 108 but left to individual states to and sectors determine where appropriate. There are some instances where it is appropriate to track individuals.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

There should not be a general right to remain anonymous or this will lead to an increase in fraud and other crime as it will be difficult if not impossible to find the perpetrators.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

This is not an issue specific to the banking sector.

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

Our members believe that for the majority of infringements, individuals look to the appropriate regulatory body to take action against the perpetrator and would not be looking for a specific ability to join in a class action (or similar) and so question whether extending powers in this way is the most appropriate way forward rather than ensuring the national regulatory bodies are appropriately resourced and have the necessary powers to take action. Any proposal relating to civil action brought through the courts would in any case have to take account of individual states' different systems of civil litigation.

We would advocate caution if the intention is to introduce multiple avenues of redress as this may be unnecessarily confusing to individuals. It is also important to ensure that whoever is involved in pronouncing judgement on data privacy matters has the appropriate expertise.

Members believe this issue is best dealt with by individual states rather than through the Convention.

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

It is difficult to see how this can be addressed through Convention 108. There are also existing requirements within the EU addressing applicable law issues. This is a crucially important issue for financial services organisations as a large proportion are multinational organisations that by their very nature operate in many jurisdictions. If a specific point is to be included on this issue, it should be ensured that it results in an improvement in the free flow of personal data, and not introduce extra jurisdictional reach.

Revisions should also take into account the broader economic benefit of those ratifying Convention 108. For example, some of our members are aware of non EU based organisations deciding not to set up processing operations within the EEA purely because EU data protection laws would have given individuals about whom personal data was being processed rights under EU law that in the circumstances were wholly inappropriate as there was no nexus between the individuals, their relationship with the organisation concerned and the EEA, and the individuals themselves have no expectation of the data protection laws of other countries applying to them.

Taking EU data protection laws as an example of the extra jurisdictional reach concern, our members believe that EU Data protection laws should not have extra jurisdictional reach, especially where an EU citizen chooses to enter into a relationship with an organisation based entirely outside of the EEA, and who of their own volition provides their personal data in order to enjoy/benefit from the provision of goods/services provided by that organisation. It is more appropriate to ensure EEA citizens have a much greater understanding of the issues so they can make an informed decision about sharing their personal data outside the EEA.

25. How to guarantee their independence and ensure an international cooperation between national authorities?

We agree that regulators should strengthen their co-operation and be able to better co-ordinate their activities to ensure consistency of implementation.

26. Should their role and tasks be specified?

Our members think that if this is to be included it should only be at a high level to cover addressing implementation and compliance.

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

The clarification and simplification of international data transfer rules, which can be particularly problematic for multinational organisations is an area members hope will be improved through revisions to the Directive 95/46/EC. In today's technological age, personal data does not only flow from A to B but is possible to be accessible from a number of jurisdictions.

There should be recognition, or at least a more practical and appropriate mechanism than the Binding Corporate Rules or Model Contractual Clauses as allowed for under Directive 95/46/EC, so that personal data can be freely transferred within group companies that are all subject to the same stringent internal policies and procedures. In these circumstances, at least, members would favour an approach which allows data sharing without the need for specific approval from data protection authorities. Outside the "intra-group" context, we have recommended that the Commission considers carefully the many circumstances in which cross-border transfers of personal data are necessary in the context of businesses which are conducted and (to a degree) regulated on a global basis and looks to adjust the regime to remove unnecessary barriers in the way of such transfers.

Greater flexibility in contractual provisions to enable transfers to countries outside the EEA, and a move away from linking specific model contracts to 'data controllers' and 'data processors' which may not be reflective of the actual nature of the relationships between parties is needed.

The Model Contractual Clauses currently contemplate one way data flows which do not reflect the current realities of cloud, on-line and distributed data processing models, making the Model Contractual Clauses inappropriate for use.

While we favour intra-group sharing without the need for prior approval, in our response to the review of Directive 95/46/EC we said that if the current model, or a similar model is to be retained, we consider that the Binding Corporate Rules (BCR) process needs to be improved with true mutual recognition, i.e. needing only the approval of the lead regulator, being the aim and organisations thereafter being accountable for compliance. The current time and cost involved in putting BCRs together threatens their very credibility and poses a significant resource burden on data privacy regulators.

Generally, the need in many circumstances (i.e. when using Model Contractual Clauses) for data controllers to obtain the prior approval of national data protection authorities before they can legitimately transfer personal data outside the EEA seems to members to be unnecessary. It is not clear what purpose the various prior approval arrangements achieve and also appear to place an

unnecessary burden on data protection authorities who are often not able to deal with applications for approval in a timely manner. We recommend that these arrangements are dispensed with.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

Our members do not believe there should be different rules for the public and private sector; existing principles are relevant to both and have the flexibility to be applied in different ways relevant to the processing. The issue of non parity of sanctions applied in practice for non compliance between the public and private sector is seen as somewhat contentious.

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

Members do not believe the role of the Committee needs to be changed.

ALBANIA - DATA PROTECTION COMMISSIONER

Object and Scope of the Convention, Definitions

1. Taking into account the primary purpose for the drafting and approval of this Convention, whereby the legislative capacity building intended by Member States under protecting the privacy of individuals due to a rapid development of technology used for processing personal data, analyzed it in 80-years, but the deal early in the 60 by some member countries and by itself the Council of Europe, remains even today a target and aim to be examined in relation to current technological developments.

   This assessment to be undertaken by the T-PD and other relevant structures of the EC should be in relation with developments with recent legislative developments in Member countries, developments which may have provided the latest technological advancements.

   We believe that only after this study can come up with a conclusion of T-PD, whether further detailed technological aspect or conventions in its entirety or to maintain simplicity. Also, we should consider the possibility that the Convention still allow its application in terms of manual processing, and in both sectors, public and private. A more detailed study of information technology experts will come to the aid assessment undertaken by the T-PD.

2. Yes, we think that the scope of this convention has tended since its design to cover as broad a right to privacy and the protection of personal data, so it will be seen to place the proposal to add a variety of definitions ranging from "The right of privacy" and "Protection of personal data" and other definitions that give a sense not only for guiding the implementation of it, but that will bring innovation in terminology and definitions set forth in this area.[245] We think that is the best case experts from T-PD have provided definitions that include situations that may create legal gaps in the implementation of this convention by member states, and to create the possibility of amendments to their legislation.

3. As above mentioned, we think that the approach to protection of privacy and personal data should guaranteed as the controllers of those public and private.

[245] The experience of EU member states in their contribution in the context of the modernization of EU legislation, such as Directive 95/46/EC and a series of other acts can be analyzed in order to modernize the Convention 108 concerning definitions that at times seem like there completed.

4. We think that should be the exception to the concept and should not cover cases of processing by individuals for personal and family life.

5. Taking into consideration the fact that the beginning of a process chain in data processing begins with "collection" and may end in "spread" or "international transfer", we believe that the list of definitions to be added to the definition of “collection”, which brings the start of the process chain contrast, if the data controller has been spread by a different controller or collected by the controller in question.

We believe that the addition of definitions, if done, should reflect the reality of cases and examples in practice, that should be eliminated or hypothetical cases that have had no special effect in the processing. The spectrum of processes could be the subject of a study of various experts, who can argue, explain, analyze for the members of T-PD concrete cases about the specifics of various sectors.

6. We think that a revised definition for the term "controller" should be part of the proposals and discussions of experts. If the restated provisions would save the general character, then a separate list of expanded criteria should be part of the “Explanatory Report." Despite this list may not be entirely exhaustive or in practice are not display cases ambiguity, we should try to create those maximum belief that which legal entities and legal terms would be considered the controller on the territory of the parties. Also, taking consideration that in specific cases may exist controllers who are responsible for the same "data files" as well as cooperation between them in processing should be provided in the definition.

Protection Principles

(7-10) Taking into consideration the fact that one of the purposes of this Convention aims at facilitating the procedures for an individual to a State Party have the right to be informed and to appeal to the connection with the processing of his data by a controller in another State Party, we think that despite the applicability of domestic legislation which operates the controller, should be included in the convention of eight (8) basic principles of the protection of privacy and personal data. These principles have been applied in Directive 95/46/EC, as the principle of proportionality and transparency in the processing, thus the right to be informed. Also the issue of legality should be treated in the convention recently.

If the modernization will be understood as maximum possible combination forecasting principles and eligibility criteria, then we think that this would remain the core of our enterprise, not given the limitations of current projections presented in the legislation of member states. On the one hand, this step must be taken to create maximum convenience on the subject of data to address a concern about its privacy and data which are processed by a controller in another state, and in turn form create a proper legal basis for the competent authorities of States Parties to provide assistance to each other.

11. Today the treatment of sensitive data as a separate category that requires more specific protection, often seen as a category are to be evaluated cannot be taken as separate from the assessment of the legality of processing and application of basic principles. It is the less possible today to draft a definitive list which specifies the data that are considered sensitive, since many countries have enhanced by some other, even further from what it defines as sensitive data the Directive 95/46/EC. Drafting a new list of sensitive data could be the subject of experts.

12. Addressing the special categories of data subjects, such as "Children" could be a step ahead of this convention, so basically less protected categories which can be more than one. But this should not be discriminatory in view of the rest of the categories. We believe that should be developed provisions of extensive character in the Convention, which could allow maximum space for States Parties to legal amendments in national legislation. Provisions related to mitigating such categories can be designed to ensure mitigation procedures under Submission of individual belonging to such categories or their legal representatives. Also, provisions can be presented mitigating actions and for providing mutual aid and assistance provided by the competent authorities of States Parties.

Also we think that, another category which may be included in this development may also be the category about data of "dead people." The discussion in this case lies in the data protection of these persons, the determination of the persons (for example: their heirs) to have the right to search over this data because of different arguments or issues or to accomplish a specific purpose, etc.

(13-16) We think that the issues of data security should occupy an important place in the provisions amending and with the assistance of experts of information technology must be provided for specific situations to prevent breach in security of data being processed. Breach of security, data processed on telecommunications, location and orientation of movement and many other forms of treatment today are finding application in many European countries where the need is demonstrated in amending the provisions of the Convention 108. Also, these provisions may also expand on the responsibilities that have processors. We think also that "notice for violating the security of data being processed" should be given not only to the data subject but also the by supervisory authorities of member countries (security breach notifications), where security breach occurs in processing.

Rights and obligations

17. The right of access should not be limited only to information given to the data subject about the category of data that is processed but also to their source if they are received by another controller. However, we can discuss the exceptional cases when this information cannot be given, for example if it cannot be given once the person is not found, whether such predictions are part of the legislation of member countries, etc. Also, the logic followed in processing will meet the right of access to the data subject, particularly in relation to automatic decision.

18. The right of opposition by the subject should be considered, but when such cases when it can exercise the right to opposition are foreseen, especially when processing is performed in the public interest. It would also be necessary to foresee the methods by which that right could be exercised.

19. We believe that the concept of "confidentiality" should be applied in cases of usage of information systems.

(20-21) In terms of new technologies used today to locate the individual, we believe that our assessment should be based on a contemporary study, as well as on an evaluation of balance between the use of such technologies in the public interest and the right of privacy.

22. Setting the right balance between information and the right of privacy is one of the topics that continue to be debated today by experts and could certainly be given place in the

process of modernization of the Convention, but will this situation be the subject of the scope of this convention, how practical would it be, and what measures have been taken so far by the state parties to fix this situation by the national legislation?

Sanctions and Remedies

23. It is clear that the possibility that this convention can give to data subjects by such class action, i.e. the consequences of breaches of data privacy and is committed to a particular area where the consequences are massive, for example in cases of direct marketing or use of profiling by large companies, would create the possibility of treatment and screening through a collective lawsuit. But also, on the other hand should be given space in the Convention and solutions through mediation mechanisms which are more rapid and effective and less costly.

Data Protection Applicable Law

24. In some countries their laws on private international law establish rules governing the applicable law on the violation of rights of personality, which can be categorized the right to privacy (for this can develop a survey). For this reason we think that it can be defined in the Convention a general rule by which states parties can foresee specific rules on the applicability of the law on data protection (jurisdiction). However in their discussion the experts could take into account the possibility of determining the rules to the Convention on the applicability of the law and jurisdiction.

Data Protection Authorities

(25-26) The issue of guaranteeing the independence of the supervisory authorities may be an issue subject to the amendments of the Convention, but nevertheless the decision remains with the Member States to ensure that status (at least for those countries whose authorities do not have this status and who may not have designated such an authority to act to the international cooperation in this field). But on the other hand the experts may draft and approve specific provisions on procedures and actions of the authorities responsible for mutual assistance.[246]

Transborder data flows

(27-29) Development of technology, as emphasized several times above, will need to accompany changes in concepts and situations that the modernization process of the Convention 108 should not bypass. Again, we are of the opinion that the T-PD experts will need to be informed by information technology professionals in order to understand the technicalities of the actions performed by the controllers, during the data transfer, and to clarify specific cases when actions on Internet would be legally considered as transfers.

Taking into consideration the fact that pursuant to the Additional Protocol to the Convention transfer to a non-member country are also allowed, as well as the fact that the Convention did not set a minimum standard rules by which to define “a country with an adequate level",

[246] We can bring into attention the Recommendation Nr. R (80) 13 “On exchange of legal information in relation to data protection’, 1980.

we think that experts would like to have a list of minimum guarantees. Directive 95/46/EC addresses the transfer and we can refer to minimal criteria provided where their own national legislation guarantees the "sufficiency" in the first place, institution building and the independence of the supervisory authority, formal guarantees that the State grants, as well as a number of other criteria laid down in Article 26 of the Directive.

The issue of adequacy may also be determined on the basis of large sectors of processing, i.e. when bilateral agreements could be the criteria for the public sector, where specific provisions on data protection are provided, as well as establishing binding corporate rules or contractual closes regarding the private sector.

The role of T-PD

30. Discussion on strengthening the role of T-PD should be assessed and coincide with the practices and the role of policies pursued by the EC in relation to committees covering various areas in the organization, but certainly some competences or the advisory role, as well as the competences of standard-setting and monitoring could be strengthened.

ARD

März 2011

Stellungnahme
der Arbeitsgemeinschaft der öffentlich-rechtlichen Landesrundfunkanstalten der Bundesrepublik Deutschland (ARD) und des Zweiten Deutschen Fernsehens (ZDF) zur

Umfrage des Europarates zur
Modernisierung der Konvention 108

Executive Summery

ARD and ZDF welcome the initiative of the Council of Europe to review Convention 108. New technological challenges and changing user behaviour require updating existing data protection rules. As public service broadcasters our main concerns in regard to a revision of the Convention are the following:

Data protection needs independent Media

It is owed to the vigilance of the media, that in the recent past a number of severe breaches of data protection rules have been made public. To continue to do so, data protection needs independent media. To fulfil its important role, public service broadcasting must rely on a data protection regime that leaves investigative journalism enough leeway to act as society's watchdog. Basic media specific requirements to do so are as follows:

- Creation of a **fair balance between the fundamental rights of privacy** (Art. 8 ECHR) **and the right of freedom of expression** and the proper working of the media (Art. 10 ECHR) to be laid down in Convention 108 by example of Art 9 (2b) Council of Europe Convention and Art. 9 EU Data Protection Directive.

- **Maintaining broadcasting specific data protection supervision**: Data protection supervision for public service broadcasting is provided by their proper independent control bodies, rather than by State authorities. On the one hand this is owed to the requirement of independence of the media laid down in Art. 10 ECHR, on the other hand, it has ensured highly effective control.

Raising citizens' awareness on how to protect their personal data

Next to the improper use of data by third parties and personal data, infringements by State authorities as well as irresponsible handling of their own data by citizens have become a growing concern. ARD and ZDF put great effort in informing and educating their audiences – especially children and young adults – on how to protect sensitive personal data while enjoying the benefits of digital media.

Minimizing the amount of data collected and limiting its use to the stated purpose

While in the context of traditional broadcasting the user always enjoyed full anonymity, this cannot be taken for granted for services provided via the Internet. In that context, ARD and ZDF support the principle to strictly limit the collection of personal data to the stated purpose.

Einführende Bemerkungen

ARD und ZDF begrüßen die Initiative des Europarates die geltende Datenschutzkonvention (Konvention 108) zu überprüfen und Überlegungen darüber anzustellen, ob sie verbessert und wo sie modernisiert werden soll.

ARD und ZDF schließen sich der Auffassung an, dass die ständig wachsenden Herausforderungen neuer Technologien eine regelmäßige Evaluierung des für einen effizienten Datenschutz nötigen Rechtsrahmens begründen. Auch die Einflüsse eines sich ändernden Verbraucher- und Nutzerverhaltens und nicht zuletzt die fortschreitende Globalisierung machen dies erforderlich.

Risiken für den Datenschutz erwachsen durch das **missbräuchliche Verhalten Dritter** (meist aufgrund kommerzieller Interessen), aber auch durch den **Staat**. Allerdings muss auch berücksichtigt werden, dass **Bürger selbst** durch ihre Verhalten datenschutzrechtlich relevante Probleme schaffen oder fördern, wenn nicht sogar auslösen. Viele geben zunehmend ihre persönlichen Daten in sozialen Netzwerken oder auf anderen Plattformen ganz offen preis, ohne sich der Folgen ausreichend bewusst zu sein.

Transparenz, Aufklärung und Schulung

Mit den traditionellen Instrumenten des Datenschutzes, insbesondere einer staatlichen Aufsicht, lässt sich dieser Entwicklung nur sehr eingeschränkt begegnen. Entscheidend ist vielmehr ein datenschutzpolitischer Ansatz, der den Bürgern Anleitungen und Instrumente an die Hand gibt, selbst richtig mit ihren Daten umzugehen. Auf diese Weise können Gefahren rechtzeitig erkannt werden, dass es erst gar nicht zu einer Preisgabe der Daten kommt. Hierfür bedarf es nicht nur größerer Transparenz bei der Datenverarbeitung. Vielmehr muss die **Aufklärung und die Schulung** im richtigen Umgang mit den eigenen Daten weit größere Beachtung finden, als dies in den existierenden Vorschriften bislang anklingt.

ARD und ZDF engagieren sich deshalb in Fragen von gesellschaftspolitischer Bedeutung und setzen sich unter anderem sowohl in ihren publizistischen Angeboten als auch ansonsten für eine **kontinuierliche Weiterentwicklung des Selbstdatenschutzes** ein.

So werden in an Minderjährige adressierten speziellen Onlineangeboten Datenschutzerklärungen für die Eltern von speziellen kindgerechten Datenschutzerklärungen begleitet. ARD und ZDF betrachten es als unverzichtbar, Kinder **altersgerecht** über Datenschutz aufzuklären. Zudem verlangt gerade der Umgang mit den Daten von Kindern ein ganz besonders hohes Schutzniveau.

Datenschutz und Rundfunkangebote im Internet

Die Fernsehnutzung hat sich in den letzten Jahren erheblich verändert. Fernsehen wird nicht mehr nur als klassischer Rundfunk konsumiert, sondern zunehmend auch über Abrufdienste im Internet. Dies stellt Rundfunkunternehmen vor neue Datenschutzrechtli-

che Fragen: Denn ein wesentlicher Vorteil des klassischen Rundfunks besteht darin, dass der **Rezipient anonym** bleiben kann, d. h. über die inhaltliche Nutzung fallen keine Daten an. Der zunehmende Gebrauch von Rundfunkangeboten über das Internet hat allerdings zur Folge, dass dieser Vorteil - technologisch bedingt - nicht erhalten werden kann.

Im Interesse der Nutzer setzen sich ARD und ZDF deswegen aktiv nicht nur für eine verbesserte Transparenz der hiervon betroffenen personenbezogenen Daten ein. Vielmehr muss auch an den Grundsätzen der **Datenminimierung und der strikten Zweckbindung** festgehalten werden.

Wächterfunktion der Medien

Nicht nur zur Aufklärung und Unterrichtung der Nutzer leisten die Medien einen Beitrag: Bekanntlich hat es in Deutschland in den vergangen Jahren **besonders gravierende Missstände** im Umgang mit personenbezogenen Daten seitens verschiedener Unternehmen (Telekom, Bahn, Discounter) gegeben. Dies hat dazu geführt, dass die Novellierung des nationalen Datenschutzrechts in wichtigen Einzelthemen auf den Weg gebracht wurde. Diese – für das Datenschutzniveau in Deutschland letztlich positive – Entwicklung beruht ausnahmslos darauf, dass Medien und deren Journalisten, darunter auch Mitarbeiter von ARD und ZDF, jene Missstände aufdeckten. In keinem der angesprochen Fälle waren es die zuständigen Kontrollstellen, die eine Ermittlung angestoßen hätten.

Die Beispiele machen deutlich, dass auch ein ausgebautes staatliches Kontrollsystem darauf angewiesen bleibt, dass die **Medien ihre Wächterfunktion** wahrnehmen und für Information und Aufklärung der Bevölkerung sorgen können. Gerade dem Rundfunk kommt dabei eine immanent wichtige Rolle zu.

Festzuhalten bleibt damit, dass der Datenschutz **unabhängige Medien** voraussetzt. Eine staatliche Einflussnahme auf die Medien - auch etwa über eine staatliche Datenschutzaufsicht - wäre damit nicht zu vereinbaren. Datenschutzrechtliche Regelungen müssen in ihrer Gesamtheit so gestaltet sein, dass sie den Medien eine effektive Wahrnehmung ihrer besonderen Aufgaben und die dafür unverzichtbaren Spielräume garantieren.

Datenschutz und Medienfreiheit

Datenschutz beruht auf dem **informationellen Selbstbestimmungsrecht** als Teil des allgemeinen Persönlichkeitsrechts. Das bedeutet, dass jeder das Recht haben soll, das Bild, das Dritte sich von ihm machen, zu steuern. Der Einzelne entscheidet nach den Grundsätzen des Datenschutzes selbst, ob er sich gegenüber der Öffentlichkeit „abschotten“ will.

Zur Freiheit der Medien zählt es hingegen, Informationen sammeln, verwerten und verbreiten zu dürfen. Mit der Information und Aufklärung der Bürger kommen die Medien ihrer grundlegenden Funktion als Faktor für die Demokratie nach. Diese Tätigkeit der

Medien ist nicht etwa dem Recht der Einzelnen auf informationelle Selbstbestimmung untergeordnet: Es handelt sich vielmehr um eine **öffentliche Aufgabe zugunsten des Gemeinwesens**, wenn Öffentlichkeit geschaffen und Meinungsbildung ermöglicht wird. Damit leisten die Medien einen entscheidenden Beitrag zur demokratischen Willensbildung wie auch generell zur Gewährleistung des gesellschaftlichen Zusammenhalts.

Notwendiger Ausgleich der in der EMRK niedergelegten Grundrechte

Neben dem Grundrecht auf Privatheit (Artikel 8) legt die EMRK das Grundrecht auf Informations- und Meinungsfreiheit (Artikel 10) fest. Eine wesentliche Forderung von ARD und ZDF ist es, die Balance zwischen diesen Grundrechten herzustellen und diese auch in der Konvention 108 zu verankern.

Ansätze für einen derartigen Ausgleich finden sich in Artikel 9 (2b) der Europaratskonvention. Demnach sind Ausnahmen u.a. „zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter möglich." In dem erläuternden Bericht hierzu wird festgestellt, dass Ausnahmemöglichkeiten im Sinne dieses Artikels unter anderem aus Gründen der Pressefreiheit gewährt werden können. Eine derartige Formulierung gibt für die Betroffenen keine ausreichende Rechtssicherheit.

Im Recht der Europäischen Gemeinschaft erfolgt die Abwägung der beiden Grundsätze sowie die daraus sicher ergebene Ausnahmemöglichkeit für Medienunternehmen in einer sehr viel klareren und eindeutigeren Art und Weise. Die Ausnahmeregelungen des Artikel 9 der EG Datenschutzrichtlinie stellt eine angemessene Absicherung der Medienfreiheit dar. Eine derartige Regelung sollte auch in die Europaratskonvention aufgenommen werden um Rechtssicherheit zu schaffen.

Datenschutzbehörden

Bei ARD und ZDF wird die Datenschutzaufsicht durch rundfunkeigene, völlig unabhängige Kontrollstellen wahrgenommen. Sie unterliegen nicht einer Aufsicht etwa durch die staatlichen Datenschutzaufsichtsbehörden. Damit wird dem Gebot der staatlichen Unabhängigkeit der Medien entsprochen, das auch dem Art. 10 EMRK innewohnt.

Diese Form der Datenschutzaufsicht hat sich als effizient erwiesen. Es ist kein einziger Fall bekannt, in dem diese rundfunkspezifische Kontrolle versagt hätte. Im Gegenteil, die speziell ausgestaltete Datenschutzaufsicht bewirkt eine **besonders enge Kontrolldichte**. Dies führt dazu, dass datenschutzrechtlich relevante Vorkommnisse sich auf wenige und allesamt wenig gravierende Fälle beschränken. Datenschutzpannen und Datenmissbrauchsfälle, wie sie in den Zuständigkeitsbereichen der allgemeinen staatlichen Datenschutzkontrolle seit Jahren leider vermehrt in Deutschland auftreten, haben sich im gesamten Rundfunksektor nicht ereignet.

ARD und ZDF plädieren deshalb dafür, bei einer Fortschreibung des Art. 13 der Datenschutzkonvention sicher zu stellen, dass weiterhin für die unter die Vorschrift des Art. 10

EMRK fallenden Rundfunkanstalten **rundfunkeigene, völlig unabhängige Datenschutzbehörden** und nicht etwa die staatlichen Datenschutzbehörden beauftragt werden.

6

BULGARIA - COMMISSION POUR LA PROTECTION DES DONNEES PERSONNELLES

Objet et champ d'application de la Convention, Définitions

1. Rédigée selon une approche « technologiquement neutre », la Convention 108 est un instrument général et simple : peut-on conserver cette approche ou doit-on au contraire élaborer un texte plus détaillé ?

We think that the Convention should offer general personal data protection and privacy framework and at the same time take into account some common problems and tendencies in these spheres, which were established in the last years, without laying down more detailed texts.

*2. La Convention 108 devrait-elle définir le **droit à la protection des données** et le **droit au respect de la vie privée** ?*

In the Convention should be determined, preferably in Art. 2 "Definitions", the concepts "personal data protection right" and "right of privacy" and their scope.

3. La Convention 108 protège les individus contre toute atteinte portée à leur vie privée par des autorités privées et publiques, y compris la police et la justice. Cette approche globale doit-elle être conservée ?

We think that privacy and data protection rights despite of existing in the legislation as separate fundamental rights are connected with each other and aside from competent authorities in the police and judicial sphere also personal data protection authorities should have the possibility to protect the individuals against intrusion in their privacy.

*4. La Convention 108 n'exclut pas de son champ d'application les données traitées par une personne physique pour l'exercice d'**activités exclusivement personnelles ou domestiques**. Doit-on maintenir cette approche, ou au contraire introduire une exception dans ce cas précis (dans le contexte spécifique du Web 2.0.) ?*

We consider appropriate from the scope of the Convention to be excluded personal data processing by individuals for personal or domestic needs. The fact cannot be avoided that technically and practically is almost impossible the relevant Internet site administrator to exercise control by the exchange of information between the site's users.
Currently, the most electronic means for direct communication, for example, forums have special codes of conduct, which if not observed lead to blocking or deletion of the relevant user.

*5. La définition du **traitement automatisé** n'inclut pas la collecte des données : le fait que la collecte fasse l'objet d'une disposition spéciale est-il problématique ? Est-ce suffisant ? Doit-on ajouter d'autres opérations à la liste existante ?*

La question de la « visualisation » des données personnelles notamment celles des scanners corporels dans les aéroports mérite réflexion. Je pense qu'on devrait considérer les images

des scanners corporels comme des traitements automatisés bien qu'il n'existe pas à proprement parler un traitement classique des données.

*La définition du **maître de fichier** devrait être revue : plusieurs critères doivent-ils être répertoriés, ces critères doivent-ils se cumuler, peut-il y avoir plusieurs maître de fichier pour un seul fichier?*

We think that the definitions "data controller" and "data processing" are very well regulated in Directive 95/46/EC and the text should be adopted from there. The same applies for the data processing criteria. It is appropriate the definition "data controller" to be extended and also to include other operations, for example data collection. Practically, there can be more that one controller of register if there is a joint activity between them (for example connecting the systems between two controllers).
There isn't explicit regulation in the LPPD of the possibility a particular register to be maintained by two controllers. There is no obstacle however if necessary, two controllers to maintain jointly a common information system (register), if this is required by their activity. Till now, CPDP doesn't have information for such practice. In cases, when two controllers use one register, for register's controller is considered only one of them (the information system owner).

*6. De nouvelles définitions sont peut-être nécessaires, comme celle du **sous-traitement** ou celle du **fabricant des équipements techniques**.*

Yes. The subsequent data processing should be regulated

Principes de protection

*7. De nouveaux principes pourraient être ajoutés à la Convention, comme le principe de **proportionnalité** qui devrait s'appliquer à l'ensemble des opérations réalisées sur les données. Ce principe est également lié au **principe de minimalisation des données** qui vise à limiter la collecte des données à caractère personnel au strict minimum, voire à y mettre un terme quand cela est possible.*

It is advisable in the scope of the personal data processing principles to be included the proportionality and data minimization.

*8. La question du **consentement** devrait-elle être envisagée en étroite liaison avec le principe de transparence et l'obligation d'informer, ou en tant que condition nécessaire à satisfaire un traitement loyal et licite avant toute autre action ?*

All data protection principles are closely connected because they constitute the lawful data protection. We think that is appropriate in all cases the consent to be connected with the transparency and informing the individuals as well to be necessary condition for data processing.

*9. La Convention 108 devrait-elle aborder la question de la **légitimation des traitements de données** comme le fait la Directive 95/46 dans son article 7 ?*

Yes, it is necessary to have clearly written parameters of lawful personal data processing similar to those of Directive 95/46/EC.

*10. La Convention 108 ne fait pas de référence expresse à la **compatibilité nécessaire entre l'utilisation des données et le but** initial de leur collecte. Or, aujourd'hui, les données à caractère*

personnel sont généralement utilisées à des fins qui vont bien au-delà de celles initialement prévues, d'où la question de la compatibilité.

The advisability should be clearly regulated as data processing principle so that the rules for personal data processing and protection, which should be observed by the personal data controllers are clear and in order to exercise effective control from the supervisory authorities in this sphere.

*11. La définition des **catégories particulières de données** faisant l'objet d'une protection accrue est très large, ce qui pourrait entraîner une application excessive de cette restriction : est-ce l'information ou son traitement qui est sensible ? Devrait-on ajouter d'autres catégories de données, comme les numéros d'identification (nationaux) et les données biologiques ou biométriques ?*

We consider necessary the sensitive data definition to be revised, following the legislation amendment process, which has begun in the European Commission. There is no obstacle the definition to be extended including biometric data. It is not clear what is understood under biological data. We don't think the identification number constitutes sensitive data.

*12. Une protection spécifique pourrait également être appliquée à certaines catégories de personnes sur lesquelles portent les données. Les **enfants,** en particulier, peuvent avoir besoin d'une protection spéciale en raison de leur vulnérabilité. Y-a-t-il un besoin de dispositions spécifiques à la protection des enfants ? Si tel est le cas, quels aspects devraient aborder ces dispositions ?*

Data about minors should not fall in the sensitive data category because the subject of rights (data subject) is not the criteria for the data sensitivity. The information itself is decisive. One and the same data for minors and adults can be defined as sensitive or not depending on their specific context. In all cases however, is necessary to think about the regulation of specific order and conditions for protection of these individuals exactly because of their vulnerability, without its qualification as sensitive data.

*13. L'article 7 de la Convention porte sur la **sécurité** des données au sens restrictif du terme, à savoir la protection contre la destruction accidentelle ou non autorisée, la perte accidentelle et l'accès non autorisé, la modification ou la diffusion. La notion de sécurité devrait-elle également inclure un droit pour les personnes concernées d'être informées des violations de la sécurité des données ?*

Yes. We think that this is relevant in accordance with the last amendments in this regard, adopted with Directive 2009/136/EC about the data protection in telecommunication sector.

*14. Il existe certains risques découlant de l'utilisation des données de **trafic et de localisation** (données techniques accompagnant une communication) car ces données peuvent révéler les mouvements, orientations, préférences et associations avec d'autres. Avons-nous besoin de règles particulières pour l'utilisation de ce type de données ?*

No. It is not necessary all exemptions and specifications to be regulated in Convention 108 because it is general act, which defines the fundamental conditions in the personal data protection field, which by rule are related to every data processing. Traffic and localization data should be subject of regulation in the relevant special European acts (Directives).

*15. Faut-il mettre en place des systèmes de **responsabilisation,** ainsi qu'une obligation de prouver que des mesures efficaces ont été prises pour garantir le plein respect de la protection des données ?*

Yes. We consider that the implementation of the accountability principle for personal data controller about the processing of the collected data by him/her will essentially improve their protection.

*16. Devrait-on appliquer le principe du « **respect de la vie privée dès la conception »** (Privacy by Design) qui vise à prendre en compte la question de la protection des données dès le stade de la **conception** d'un produit, d'un service ou d'un système d'information ?*

Yes, but in order to effectively apply this principle it is good to be inserted personal data controllers obligation to perform risk assessment about the privacy of the individuals, whose data are processed.

Droits – Obligations

*17. Le **droit d'accès** ne devrait pas se limiter aux données mais devrait couvrir l'accès à l'origine des données, c'est-à-dire la personne qui est à l'origine de la communication. Ce droit devrait-il également couvrir l'accès à la **logique** du traitement ?*

Yes. It is very important for the individuals to be acquainted with the purposes, for which their personal data is processed and their lawfulness.

*18. Le **droit d'opposition** se justifie dans les cas où le traitement des données ne repose pas sur le consentement de la personne concernée. Le lien entre droit d'opposition et droit à l'oubli pourrait être examiné, ainsi que la possibilité de garantir le respect et l'exercice de ce droit.*

The right to object to the personal data processing can be exercised by every individual, who believes that his/her data are processed illegally. The connection between the objection and the right to be forgotten (i.e. data deletion) consists in the dropping out of the relevant personal data processing purpose. The first case concerns individual's allegation, and in the second is available proven (with facts) drop out/exhaustion of the processing purpose.

19. Devrait-il y avoir un droit qui garantisse la confidentialité et l'intégrité des systèmes d'information ?

Yes. The guaranteeing of the confidentiality and the integrity of the information systems, containing personal data, are closely connected with the providing of information security, set in Art. 7 of the Convention.

20. Faudrait-il introduire le droit de tout individu à « ne pas être localisé / tracé» (identification RFID) ?

Yes. Individuals' localization data can be obtained only in cases set in Directive 2006/24/EC and are not to be processed on common ground.

21. Les utilisateurs des technologies de l'information et de la communication devraient-ils avoir le droit de rester anonymes ?

Yes, as far as they don't perform actions which violate the legislation and the other users' privacy.

22. La Convention 108 devrait-elle aborder la question du juste équilibre entre la protection des données à caractère personnel et la liberté d'expression (nouveau concept de la presse et du journalisme dans le contexte du Web 2.0.) ?

Yes. The usage of Internet means for disseminating journalistic information always have to be balanced by taking into account the interested individual's privacy right.

Sanctions et recours

23. Devrait-on introduire des recours collectifs dans la Convention ? Faut-il examiner l'introduction d'autres mécanismes de règlement des litiges ?

Yes. Every possibility for settling personal data protection disputes, which could facilitate the individuals by the application of their rights, should be studied.

Droit applicable en matière de protection des données

24. Doit-on envisager une règle qui déterminerait le droit applicable au traitement des données (dans les cas où différentes juridictions sont concernées) ?

Yes. The regulating of the applicable law for data processing is very important for the effective individuals' protection especially by data transfer to third countries with inadequate protection level.

Autorités de protection des données

25. Comment garantir leur indépendance et assurer une coopération internationale entre les autorités nationales ?

The requirements for the data protection authorities' independence should be straitened and not only should their institutional and functional independency be set, but also the financial independency by the execution of their competences. With regard to the international cooperation between the data protection authorities the possibility of conducting of joint investigation on data protection cases outside of the territory of particular member-state could be discussed, but only as far as these actions will not present ungrounded administrative and financial burden for the data protection authorities.

26. Faut-il spécifier leur rôle et leurs missions ?

Yes. Detailing the authorities' role and tasks is done with the purpose of avoiding the ungrounded burdening of their work.

Flux transfrontières de données

27. La Convention 108 avait pour but de concilier la protection effective des données et la libre circulation de l'information sans considération de frontières. Ces principes ont été développés plus avant dans un protocole additionnel (STCE 181, 2001). En principe, un niveau de protection adéquat doit être assuré.

The guaranteeing of adequate data protection level is main requirement for trans-border personal data movement and in this connection the necessary legal provisions should be foreseen.

28. Doit-on entièrement réexaminer la notion de « flux transfrontières de données » à l'heure d'Internet, où les données circulent instantanément à travers les frontières ? Serait-il utile de fixer des règles minimales internationalement reconnues pour garantir le respect de la vie privée sans considération des frontières ? Quel pourrait en être le contenu ?

We think that, it will be useful to be determined the main rules for observing the privacy and data protection, which should have international application outside the scope of the existing ones.
In all cases, the information exchange performed by the Internet network should be well analyzed. The content should be well considered and discussed and should offer improvement of the existing legal regulation, taking into account the technology and electronic developments and the data exchange performed by specialized authorities, for example these, which operate in the framework of police and judicial cooperation.

29. Doit-il y avoir des règles différentes pour le secteur public et le secteur privé ? S'agissant notamment du secteur privé, doit-on avoir davantage recours à des règles d'entreprise contraignantes, éventuellement associées à un système de responsabilisation du destinataire final pour garantir le respect de ces règles ?

We think that data protection rules, including the accountability, should be the same for the controllers in the private and public sphere. The introduction of accountability for controllers by the requirements' infringement should be accompanied by the relevant adequate sanctions, which guarantee the effective individuals' protection by the violation of their rights.

Rôle du comité consultatif

30. La Convention 108 a créé un comité chargé de faciliter son application et, le cas échéant, de l'améliorer. Doit-on renforcer le rôle jusqu'ici principalement consultatif du comité ? Si oui, quelles fonctions faut-il développer plus avant : l'activité normative, le règlement des litiges, le suivi ?

With regard to the extension of the scope and the supplement of the Convention 108 is not necessary the role of the foreseen Committee to be increased.

CEA

Position Paper

CEA contribution on the Modernisation of Convention 108

CEA reference:	SMC-LEG-11-033	Date:	10 March 2011
ID Number:	33213703459-54		
Contact person:	Lamprini Gyftokosta	E-mail:	Gyftokosta@cea.eu
Pages:	10		

Introduction

The CEA, the European insurance and reinsurance federation, welcomes the opportunity to contribute to the consultation on the modernisation of Convention 108 that has been launched by the Council of Europe.

The CEA promotes the idea that as many countries as possible (also non-members of the Council of Europe) adhere Convention 108, so as to extend the field of equivalent legislation.

Object and Scope of the Convention, definitions

1. **Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?**

   The Convention came into force before the beginning of the Internet era and the rapid developments in information and communication technologies. The technologically neutral, principle-based approach that was introduced in 1981 stood the test of time. Since technological evolution is continuous and fast, the CEA believes that the Convention should be kept technologically neutral, to avoid being out of date every time something new emerges from the field of communications and technology.

   This view is also supported by the European Commission (EC) in its recent Communication on "A comprehensive approach on personal data protection in the European Union" in relation to Directive 95/46 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data". It would be prudent if the Convention, having a broader geographical and material scope than the Directive 95/46/ EC, kept the same approach.

2. **Should Convention 108 give a definition of the right to data protection and privacy?**

   -

CEA aisbl
Square de Meeûs 29, B-1000, Brussels
Tel: +32 2 547 5811 • Fax: +32 2 547 5819
www.cea.eu

© Reproduction in whole or in part of the content of this document and the communication thereof are made with the consent of the CEA, must be clearly attributed to the CEA and must include the date of the CEA document.

3. **Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?**

   According to article 3 paragraph 1, Convention 108 applies to the public as well as the private sector. The CEA thinks that this approach should be retained. For private authorities, because most of the international data traffic occurs in the private sector; and for public authorities, because they have to comply with their members states' data protection legislation when processing public files, even within their national borders.

4. **Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0)?**

   It should be noted that it is not clear what the question refers to when it mentions "purely personal and household activity". If it means that the process forms part of the private or family life of a natural person, Convention 108 should exclude of its scope data processed by a natural person in the course of a purely personal or household activity, as in article 3 paragraph 2 of the Directive 95/46/EC. Members States should be prevented from deciding autonomously on this matter.

5. **The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?**

   The Convention should include a definition of "processing" as in the Directive 95/46/EC where a broad set of operations performed upon personal data is included. More particularly:

   Article 2 (b) :"processing of personal data" ("processing") shall mean any operation or set of operations which is ***performed upon personal data****, whether or not by automatic means, such as* ***collection, recording, organisation, storage, adaptation*** *or alteration, retrieval,* ***consultation, use, disclosure by transmission,*** *dissemination or* ***otherwise making available, alignment or combination, blocking****, erasure or* ***destruction***".

   It would be beneficial to have consistency of approach between the Convention and the Directive in order to make the international data processing easier. This means that "collection of data", which is a key operation that marks the start of the automatic processing should be included in the definition.

   Moreover, as stated in section 4.4(a) of the Recommendation No (2002) 9 "*on the protection of personal data collected and processed for insurance purposes*", insurance undertaking must collect personal data to issue insurance policies. For this reason and in order to clarify the normal data processing of insurance undertakings, Convention 108 should include the concept of collection of data in the automatic processing definition.

   It could also be useful to include in the definition the operation of "disclosure by transmission" – that is a fundamental operation for the treatment of personal data – is part of the treatment itself, as is the case for Directive 95/46/EC and in the national legislation.

   The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

   The Convention should include the same definition of "controller of the file" as in the Directive 95/46/EC where several criteria are listed. More particularly:

   "controller of the file" shall mean the natural or legal person, public authority, agency or any other body ***which alone or jointly with others*** *determines the purposes* ***and means*** *of the processing of personal data;"*

A review of the definition of the controller of the file is desirable, especially for the facilitation of data flows within insurance groups, between direct insurance and reinsurance companies and for the shifting of tasks towards service providers.

Moreover, if the involved companies are defined as one controller of the file, the delegation and centralisation of services tasks within a group can also be facilitated. Besides, tasks have to be outsourced to competent service providers to achieve synergies and to meet the requirement of economy.

This should also be facilitated under certain legal requirements, for instance:

- if it is ensured that the data are processed only in line with the original purpose
- that the other companies have been selected carefully taking into account the appropriateness of the technical and organisational measures taken by them with respect to data protection and data security and
- if, it has been agreed in the contract that the other company offers the same guaranteed of the protection of confidential information and data protection as the insurance company itself

6. **New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.**

-

Protection principles

7. **New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.**

The principles of proportionality and data minimisation are already implemented in article 5 (b) and (c) of Convention 108: *"Personal data undergoing automatic processing shall be: (...) b. Stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. Adequate, relevant and not excessive in relation to the purposes for which they are stored (...)".*

It should be noted that the existing EU legislation requires the insurance industry to collect certain data in order to carry out its business. For example, the anti-money laundering (AMDL) legislation requires insurers to verify the accuracy of certain personal data, eg the identity of the policyholder/ beneficiary, the origin and destination of the funds. It is important that new provisions on proportionality and data minimisation do not hinder the fulfilment of existing requirements. In order to ensure the necessary flexibility for companies, any principles of data economy should, if possible, not be designed as an obligation, but as a target.

The insurance industry complies with these requirements. However, for the assessment and calculation of an individual risk, insurance companies need comprehensive information, so that the community of insured people is not unnecessarily put at a disadvantage due to bad risks.

8. **Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or a necessary condition to a fair and lawful processing, to satisfy before any step?**

When considering consent expressed and implied, the Consultative Committee should take account of the importance of tacit consent, given through concrete unmistakeable behaviours. For data flows which are necessary for the conclusion and fulfilment of the insurance contract, the instrument of consent should not be the only solution

Moreover, the voluntary nature of such declarations could at times be contested because the persons concerned need the insurance cover. Given the extent of data processing in insurance companies, systematic express consent would be burdensome. Any provision in the Convention should allow for changes in corporate structures, requiring data processing in different companies of an insurance group and the outsourcing of activities specialised external companies or persons.

The CEA understands that data subjects should be well and clearly informed in a transparent way. Nevertheless, the Consultative Committee should give more details and clarify the meaning of "*necessary condition to a fair and lawful processing that should be satisfied before any step is taken*".

9. **Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?**

Convention 108 is not compulsory as Directive 95/46/EC and this is why a detailed legitimate processing could not be efficient. Particularly with regard to a preferable accession of non EU-countries to Convention 108 a list of legitimate grounds might be too restrictive and will therefore reach little acceptance. Moreover, if the legitimate processing is defined in the convention, proportionality and tacit consent should also be included.

10. **Convention 108 does not expressly mention compatibility in relation to purpose. In today's context personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection**.

It could be useful to mention the principle of compatibility in Convention 108 in order to better clarify the limits to comply with treating personal data.

Changing the data processing goal and purpose has to be also possible, in case when an insurance company as data controller can legally justify this new purpose. For example, when law changes the data acquired by an insurance company 10 years ago may be now further processed not for the primarily goals only (eg limited to servicing the insurance processes), but may be even required for new purposed like preventing and detecting terrorism and money laundering. Additionally, the customer's right to be additionally informed should be by definition disabled in cases when there is legal provision to process this data.

11. **Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?**

As the Consultative Committee looks into the issue of special categories of data in more detail, any changes to existing categories must be carefully considered. More particularly, further details on the precise scope of data categories that could be included are required in order to check to which extent they overlap with existing categories of special/ sensitive data or if they are covered by other national or European legislation. This would indeed be essential to assess the magnitude of any such change and the potential impact it can have on both consumers and the insurance industry. Other data should only be subject to the strict safeguards if they are actually comparably sensitive.

If the Consultative Committee wants to include biological or biometric data in the "special category of data", it should ensure first that characteristics such as gender and age, that are visible to everyone, cannot be part of them. Otherwise, the definition will be incompatible with the provisions of other pieces of European or national legislation.

For instance, the Anti-Money Laundering Directive (AMDL) requires insurers to collect and process numerous data such as the identity (including age and gender) and the financial information necessary to redraw the

origin and destination of the funds. Moreover, for the conclusion of insurance contracts such as life insurance contracts, age is necessary information.

Due to the complexity of the issue and the divergencies between Contracting States, the CEA supports paragraph 48 of the explanatory report of the Convention 108 that says that *"the list of this article is not meant to be exhaustive. A Contracting State may in conformity with Article 11, include in its domestic law other categories of sensitive data, the processing of which is prescribed or restricted. The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned"*.

12. **A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?**

The main objective should be to strengthen the media competence and data protection awareness of minors, especially if these are active on the internet – in social networks, blogs and chats – and disclose information there. If the Council of Europe takes the European Commission's idea of an age limit into consideration, an age limit of 18 seems appropriate to ensure conformity with regulations of contract law if parents conclude an insurance contract for their child, the collection and processing of the data which are required for the proper initiation, fulfillment and settlement of the contract must retain possible.

13. **Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?**

The CEA believes that only breaches that pose a significant risk of harm to data subjects – and where the data subjects should take action (eg to prevent identity theft) or remain vigilant – should be notified. If the risk of harm is limited, the benefit that the data subject will gain from the notification will be also restricted and cause unnecessary stress. It might also lead to consumer apathy, which is the case in the US where so many notifications were received that significant ones were overlooked. A future provision might only interfere if particularly sensitive data are affected and if there is a risk of severe impairments of rights or legitimate interests of the data subjects

Experiences from the American market show that imposing on data controllers a duty to obligatory inform customers on information security breaches concerning their data processing is counterproductive and even erroneous, as it may result in information chaos and encouraging customers to set additional claims against insurance companies on these grounds.

14. **There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?**

-

15. **Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?**

The CEA believes that accountability systems are already in place and this is why a further introduction of accountability mechanisms is not necessary.

For instance in the UK, the Information Commissioner's Office (ICO) maintains a public register of data controllers. Each register entry includes the name and address of the data controller and details about the

types of personal information they process. Individuals can check the register to find out what processing of personal information is being done by a particular data controller. Moreover, many DPAs – including the ICO – have a full suite of sanctions available to them in the event that a data controller commits an alleged breach of the legislation. This is also the case for IT and ES.

More particularly, the Spanish Data Protection Agency has the same public and private files registry which is mandatory (if not, is an infringement of the data protection regulation) for every public or private person who processes personal data and for every file that they process.

Furthermore, in ES there is a possibility of registering to Standard Code on personal protection (developed under section 27 of the Directive 95/46/EC) which should be approved by the Spanish Data Protection Agency first. It guarantees that undertakings associations or public bodies who adopt it will assume good practices, transparency, security measures and responsible use of the personal data in his data processes. The adhesion is binding for the parties, aiming at guaranteeing that members of the Standard Code comply with it.

Additionally, in the UK, the ICO has introduced a voluntary "Personal Information Promise" which is intended to help strengthen public trust and confidence in the way that organizations handle their personal information. It is a clear statement from the very top of an organization that it values the personal information entrusted to it and will put the appropriate recourses in place to look after it. It is also sends a clear signal to the workers in the organization about the importance of looking after people's personal information and that this is something taken very seriously at senior level.

The "Personal Information Promise" does not create additional legal obligations. It reflects existing legal obligations in the Data Protection Act and puts them into straightforward language that individuals can readily understand. What it does do is to show a public commitment by the organization to comply and put in place the measures that help ensure that it complies.

16. **Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?**

When introducing new technologies, every company has to ensure that these are consistent with data protection standards. In this respect, the focus should be on the objective to design programs and procedures in such a way as to ensure that data security is ensured. At the same time, requirements that put an enormous cost burden, especially on small companies which would ultimately be squeezed out of the market, should be avoided.

"Privacy by design" has already been promoted by the ICO in the UK. While it is not compulsory, privacy by design is already encouraged.

Rights – Obligations

17. **The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?**

The CEA believes that the data subject should have the right to access data. A right to know the source of data might be relevant to the area of advertising where data are disclosed repeatedly and where it is no possible to identify the body which originally collected the data. Nevertheless, it should be borne in mind that sometimes, the request for access can be frivolous because the data subject is only motivated by willingness to control the processing rather than to confirm the accuracy of data held. Therefore, when considering a less

limited right to access, the access to data should not cover the logic of the processing. Moreover, access to the logic of the processing should not be envisaged under Convention 108.

In the UK, it is a requirement of the 1st data protection principle (fair obtaining/lawful processing) that data subjects be told the sources (or origins) of data, as well as the uses and disclosures. Where a data controller uses a decision-making process that operates automatically and is the sole basis for any decision (eg credit scoring), the data subject is entitled if they so request to receive information as to the logic involved in the decision-making. But in disclosing this information, the data controller is not required to disclose any trade secrets.

In IT as well, the data subject has the right to obtain the indication of the logic involved in case of personal data processing carried out by means of electronic tools with prior exercise of the right of access.

In ES, access to the logic of the process is part of the access right. However, in order to prevent administrative burden and excessive cost for the data processors, the data subject must demonstrate a legitimate interest under the Spanish regulation.

18. **The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.**

When the data controller processes the information legitimately under an existing exemption, the data subject should not be able to oppose the processing.

The Council of Europe should keep in mind that there are legal requirements in certain sectors which oblige the firms to collect certain data as proof of financial status. The right of opposition could be introduced as in Directive 95/46/EC when permit data processing.

The same reasoning will occur with the right to oblivion since the data should be kept by firms until the end of the contract and for legal purposes (eg keeping a document as a proof for potential litigation) or legal duties to preserve records, such as according to regulations of commercial and tax law. A right of oblivion may be addressed, if at all, in connection with the use of social networks on the internet.

Data should be kept for as long as it is relevant and for evidential purposes. This period will often be linked to the statute of limitations in each member state.

19. **Should there be a right to guarantee the confidentiality and integrity of information systems?**

-

20. **Should a right "not to be tracked" (RFID tags) be introduced?**

-

21. **Should everyone have a right to remain anonymous when using information and communication technologies?**

-

22. **Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?**

-

Sanctions and Remedies

23. **Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?**

The CEA believes that class actions should not be introduced in the Convention. The nature of these sanctions and remedies should be determined by member states' national legislation. But, in any event, it should be borne in mind that earlier this month, the European Commission (EC) launched a consultation about adopting a more coherent approach to collective redress by identifying common legal principles. The EC is exploring whether collective redress should be extended to new sectors. We suggest that any consideration of whether class actions should be introduced into Convention 108 would need to be discussed in the context of the EC consultation.

Class actions make sense only if no data protection authority is designated and no other protective mechanisms exist. For instance, supervisory authorities according to Directive 95/46/EC have extensive powers, and may act not only upon requested of data subject but also ex officio.

It should be borne in mind that the European Commission launched a consultation about adopting a more coherent approach to alternative dispute resolution (ADR) mechanisms by identifying common legal principles. This is why the CEA believes that any discussions related to ADR should be discussed in the context of the EC consultation.

In the offline area instead, out-of-court possibilities for dispute settlement should be developed as a matter of priority. For instance, the German insurance industry has gathered positive ombudsman for insurance, a neutral and independent arbitration board, which works free of charge for the consumer and enjoys wide acceptance among customers.

Data protection applicable law

24. **Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?**

Given the increased complexity caused by globalization and technological advances (eg cloud computing) the CEA believes that there is a need to clarify requirements around applicable law. This is necessary, not least to reduce risk of forum shopping and the compliance burden imposed on firms.

Especially, in case of cross-border data processing, the determination of applicable law might be problematic. At EU level, this would be due to the differences in the implementation of the data protection directive amongst member states. This may also be due to the fact that data protection authorities apply different standards in interpreting these provisions, especially in terms of security measures that must comply with the data recipient, related with the computer or paper files of personal data.

One of the revised Convention 108 must be solve this problem of applicable law to data processing, by promoting the international cooperation and guidelines on data protection issues and rules between the countries.

Data Protection Authorities

25. **How to guarantee their independence and ensure an international cooperation between national authorities?**

-

26. **Should their role and tasks be specified?**

The CEA does not support this suggestion as this matter falls within the national authorities; responsibilities. Their role and tasks must be addressed by the national rules and regulations of each data protection authority.

Transborder data flows

27. **The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.**

The CEA favours steps towards the facilitation of international transfers and free flow of information regardless of frontiers by Convention 108, as it is enshrined in Article 10 of the European Human Rights Convention. As it is enshrined in Article 10 of European Human Rights Convention, the international transfer of data should assume the same level of protection from a country to another one.

Personal data protection is equally important to the correspondents of MTPL insurers, the Green Card Bureaux, Motor Guarantee Funds and Compensation Bodies, which handle insurance claims on a daily basis and which must transfer personal data in an international context in order to meet with their responsibilities.

28. **Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?**

It would be important and useful to promote codes of conduct concerning cross-border transfers of data, ensuring that every code is accepted and registered by all relevant data protection authorities. It will also be very useful to establish minimum international rules of international data transfers, especially in the insurance market, which have a continuous data flow and can operate in many countries at the same time and must comply with very different data protection legislations.

The Consultative Committee should take into account section 12.2 of Recommendation 2002 No 9, relating to "transborder data flows" which states that the insurance undertakings, which belongs to Contracting States of Convention 108, and are from countries that guarantee an adequate level of protection, must not be imposed to special conditions of privacy related to "transborder data flows".

29. **Should there be different rules for public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?**

The CEA believes that the legislation should be applicable equally to both public and private sectors. However, national DPAs should have the right to consider whether these sectors should be treated differently in certain circumstances. By the way of example, in the UK, the Information Commissioner adopts a different approach to auditing of public bodies (compulsory) and private bodies (consensual).

Moreover, Convention 108 may foster the resource to ethic codes, above all in case of multinational groups. However, it should be noted that any violation to data protection can be exclusively ascribed to the company exerting the violation unless a provision by a national law or an agreement between the parties be envisaged.

Already according to Directive 95/46/EC, the stipulation of BCR is a way to legitimise international data flows. An important aspect is the practicability of authorisation procedures. This includes recognition of the

authorisation granted by one data protection authority by other authorities to avoid multiple cost-intensive and time-consuming inspection effort.

Role of the consultative committee

30. **Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?**

Should the role of the consultative committee be strengthened, this should only be in relation to monitoring functions.

The CEA is the European insurance and reinsurance federation. Through its 33 member bodies — the national insurance associations — the CEA represents all types of insurance and reinsurance undertakings, eg pan-European companies, monoliners, mutuals and SMEs. The CEA represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers generate premium income of over €1 050bn, employ one million people and invest more than €6 800bn in the economy.

www.cea.eu

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is a law and technology clinic based at the University of Ottawa in Canada. CIPPIC's advocacy covers diverse technology-related issues, and has been advocating in the public interest on privacy issues since its inception. CIPPIC's experience in this area includes, but is not limited to, testimony before Canadian parliamentary committees on privacy-related legislation including active participation in a review of Canada's federal data protection statute, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), intervention before the Canadian judicial system on various privacy related issues, and provision of legal assistance for under-represented Canadians on privacy issues.

In addition, CIPPIC has filed over 20 privacy complaints under PIPEDA on data protection matters such as the privacy practices of social networking sites, the use of mid-network collection of data on customers by Internet Service Providers for the purpose of traffic management using Deep Packet Inspection tools, the implication of online data breaches of sensitive data, the cross-jurisdictional data collection practices of US-based websites and web-based services, and the potential privacy implications of the Google/Double-Click merger, to name a few.

CIPPIC is in receipt of comments submitted to the Council of Europe by Nigel Waters and Professor Graham Greenleaf on behalf of the Cyberspace Law and Policy Centre (CLPC) as part of this consultation. CIPPIC offers this submission in support of those comments and to offer our experience with Canada's data protection regime in aid of the Council's efforts at reviewing its Convention 108. Many of our comments are based heavily on those of the CLPC submission and where we fail to expressly comment on specific elements of that submission, we can be taken to be supportive of those elements. We structure our submission around the general questions in the Council of Europe "Modernisation of Convention 108: Give Us Your Opinion!" document.

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

A principled, technologically neutral approach is preferable. PIPEDA is drafted in a flexible manner that has allowed it to remain relevant in an era where the rate of technological change has been perhaps unprecedented and continues to increase. A flexible, principled approach is essential, but needs to be updated from time to time to address some shifts in practices and technologies.

2. Should Convention 108 give a definition of the right to data protection and privacy?

Many have struggled to define 'privacy' in different ways and in different contexts. Privacy is, in CIPPIC's view, a human right best defined within the context of human rights instruments and applied to the specific context and protections set out in the Convention.

In this respect, the CLPC recommendation to define privacy rights in broad strokes within the Convention itself should be followed.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes. While Canada has taken a bifurcated approach to privacy protection vis-à-vis the public and private sectors, this has been criticized. Particularly, Canada's Federal *Privacy Act*, which offers Canadians added privacy protection against the state, has been criticized by civil society and our Federal Privacy Commissioner for failing to remain relevant where it fails to follow the principled approach adopted in PIPEDA. Canada operates under a federal system and a number of Canadian provinces have adopted principled public-sector privacy statutes that have proven more flexible and capable of keeping up with the times.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0)?

CIPPIC shares concerns stated in the CLPC submission with respect to this question. PIPEDA is limited in its application to 'commercial activity', defined broadly. While it is able to capture Web 2.0 activity, this is only at the intermediary/organizational stage. This has been recognized as one of the coming challenges for PIPEDA's ability to protect privacy in an increasingly participative web. At the same time, it is recognized that data protection principles will be difficult for individuals acting in pursuit of private activity to meet and that, if applied to such activity, careful balancing against the free expression rights of individuals will be required. Courts may be best placed to apply evolving norms to this space, but, as noted in the CLPC submission, tribunals are of lower cost and may be able to contribute to this evolving field in a more flexible manner.

5. The definition of automated processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

   The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

CIPPIC is supportive of the CLPC submission on these points. Particularly, clarification that all collection processes should be minimized as much as possible to necessary purposes and should be conducted by non-intrusive means is integral.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

CIPPIC supports the CLPC's call for a flexible approach that emphasizes proportionality and reasonable expectations. Consent can play a role in this framework but should be adopted with caution. Consent-based protections should be coupled with specific requirements to detail intended collection, use and disclosure; to minimize such collection, use/disclosure to what is necessary for specified purposes/uses; to a right of opposition/opt-out/opt-in for secondary purposes to avoid tied-selling, and guidance on the form of consent to be utilized when acquiring consent to address consent viscosity in user interface or a strict notification-based regime where notice to unexpected or sensitive data practices is buried in long, rarely read policies.

The form and acceptability of consent should be informed by reasonable expectations and proportionality, as well as the sensitivity of the information in question, and it should be recognized that consent is not definitive in all circumstances. In addition, data controllers should not be permitted to rely on consent in circumstances where it is unreasonable to believe that individuals have provided it on an informed basis.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Data breach notification requirements are crucial for a number of reasons. First and foremost, it is important for individuals to be aware that a breach has occurred so that they are able to take steps to reduce potential harms, where necessary. Second, without such requirements, particularly backed with potential fines for non-compliance, incentive to disclose data breaches is minimal. Finally, breach notification requirements have the tertiary effect of providing strong incentives to strengthen security measures as well as an opportunity to study how and where breaches occur.

The CLPC submission properly stresses that notification requirements should be guided by specified threshold criteria. To balance the need to provide certainty in light of subjective criteria with the need to avoid notification fatigue, some have suggested a two-tiered reporting system, with a low threshold for reporting to a data protection authority and a higher threshold for reporting to affected individuals.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

The CLPC submission properly notes that a flexible regime should be able to account for the additional sensitivity and expectations raised by this type of data and to provide added protection in kind.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Accountability is an important element of any data protection regime but should not, as stated in the CLPC submission, be capable of overriding other requirements.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Specific requirements of proactivity in architectural and product design so as to account for privacy concerns is integral. More important is a commitment to 'privacy by default' as an overriding design principle. CIPPIC notes the CLPC's caution in ensuring that data protection authorities do not compromise their ability to provide *ex post* criticism by adopting an overly proactive prior approval process.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

Yes. The right to access needs to be expanded in light of the increasing complexity of computational models on which criteria and assumptions are based.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

PIPEDA's reasonable retention requirements which require personal information be made inaccessible once the purpose for which it has been collected has expired are an important part of the overall principle of minimization, limitation, and proportionality. PIPEDA additionally includes a right to opt-out of unnecessary purposes for the collection, use and disclosure of personal information.

A right to be forgotten is becoming more important in many contexts and deserves further exploration in light of the potential practical obstacles attached to its realization.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

20. Should a right 'not to be tracked' (RFID tags) be introduced?

Both of these rights can be achieved through more general principles of confidentiality, privacy, and accuracy.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

Anonymity is a right that deserves distinct articulation and protection. The capacity to act anonymously is central to protection of privacy in inherently public/semi-public spaces such as those that are pervasive online. It is also integral to the minimization/limitation principle and at the core of proposed federated identity systems. Yet incentives are strongly aligned to require identification in situations where it is not necessary. The language proposed in the CLPC submission is instructive.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

As noted in the CLPC submission, additional balancing of free expression (beyond that already inherent in conceptions of reasonableness and proportionality) is more appropriate where individual activity such as citizen journalism is covered by the Convention. Even in such contexts, care must be taken as it will be difficult to capture the appropriate balance between expressive activities and privacy in a categorical manner. Even 'news reporting' may amount to an invasion of privacy where the public importance of the news is low and the level of invasiveness is extremely high.

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

Expanding the scope of available remedies can only further the scope of protection offered. The CLPC paper notes that remedies are available only in contexts where requests for correction have been denied. It is appropriate, in CIPPIC's view, to add fines as well as civil and class action remedies for breaches of the principles in certain contexts. ADR mechanisms could be beneficial but should not operate to frustrate other available remedies.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

A choice of laws provision will provide certainty, but should not operate to frustrate locally offered consumer protections. A place of purchase or place of sale default jurisdictional rule should also be applied with caution, taking into account the limited means of individuals, as opposed to organizations, to bring complaints in distant jurisdictions.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

26. Should their role and tasks be specified?

The points made in the CLPC submission on the role of DPAs are directly on point and particularly the requirements for statistical reporting mechanisms and provision of objective reasoning for decisions. Thought might be given to making DPA decisions binding by common law concepts of *stare decisis*.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

CIPPIC mirrors concerns stated in the CLPC of a potential 'race to the bottom' that may result from any global effort to establish minimum rules. This applies to both private and public sectors.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

CIPPIC has no comment on this point.

CNIL

Objet et champ d'application de la Convention, Définitions

1. Rédigée selon une approche « technologiquement neutre », la Convention 108 est un instrument général et simple : peut-on conserver cette approche ou doit-on au contraire élaborer un texte plus détaillé ?

Il est extrêmement important en effet de conserver l'aspect « technologiquement neutre » de la Convention 108. C'est cette neutralité technologique qui permet et qui permettra à la Convention 108 de s'adapter, sur le long terme, aux évolutions technologiques.

Par ailleurs, la Convention 108 doit rester un texte général et simple, et ce notamment pour permettre une adhésion plus large de pays du Conseil de l'Europe qui n'ont pas encore ratifié cet instrument ou de pays tiers au Conseil de l'Europe.

Toutefois, il serait utile de continuer à détailler plus avant les principes généraux de la Convention dans des textes spécifiques, notamment dans le cadre de recommandations du Comité des ministres.

2. La Convention 108 devrait-elle définir le droit à la protection des données et le droit au respect de la vie privée ?

Il apparaît avant tout utile de conserver les définitions de certains termes, notamment celles de « donnée personnelle », de « fichier », etc…

Certaines notions pourraient toutefois être révisées. Par exemple, la notion de fichier. De façon plus générale, il faudrait revoir les dispositions évoquant les fichiers automatisés ou non de traitements.

Il serait, de plus, utile d'étendre la définition de donnée à caractère personnel pour bien préciser la notion d'identifiabilité afin de préciser, comme dans la Directive 95/46/CE, qu' « *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*».

Par ailleurs, par souci de cohérence avec d'autres instruments juridiques, le « maître du fichier » pourrait devenir le « responsable de traitement ». La définition pourrait là aussi être revue pour viser l'organe qui détermine « les finalités et les moyens » du traitement. 2 En revanche, il paraît moins impérieux de définir le droit à la protection des données ou le droit au respect de la vie privée, et ce d'autant plus que ces notions pourraient être interprétées de façon évolutive, et dans d'autres contextes concernant la vie privée, à l'aune de la jurisprudence de la Cour européenne des droits de l'homme. Par ailleurs, la notion de vie privée semble, sous divers aspects, sortir du champ d'application de la protection des données personnelles (droit à l'image, secret des correspondances, protection du domicile, etc…).

Enfin, d'autres termes pourraient être définis dans la Convention 108. Par exemple, la notion de communications électroniques ou encore d'autres notions figurant dans la Directive 2002/58/CE révisée.

3. La Convention 108 protège les individus contre toute atteinte portée à leur vie privée par des autorités privées et publiques, y compris la police et la justice. Cette approche globale doit-elle être conservée ?

Il apparaît essentiel de conserver un instrument juridique unique qui contiendrait des règles générales applicables également à la police et à la justice. En effet, bien que des règles particulières doivent être prévues pour prendre en compte les spécificités des traitements mis en oeuvre à des fins répressives, il convient que la mise en oeuvre de ces traitements soit soumise aux mêmes principes généraux en matière de protection des données. En particulier, des limitations au droit à l'information et au droit d'opposition des personnes concernées devraient être mises en place, de même que des aménagements aux modalités d'exercice des droits d'accès et de rectification de ces personnes, qui pourraient par exemple être exercés de manière indirecte.

Ce caractère général de la législation en matière de protection des données se retrouve d'ailleurs dans la législation française, ainsi que dans les projets de refonte du droit communautaire en la matière. Ainsi, la CNIL est pleinement compétente pour exercer ses pouvoirs de contrôle *a priori* et *a posteriori* sur les fichiers de police, y compris ceux du secteur de la défense et de la sûreté de l'Etat, pour lequel certaines règles ont cependant été aménagées.

4. La Convention 108 n'exclut pas de son champ d'application les données traitées par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. Doit-on maintenir cette approche, ou au contraire introduire une exception dans ce cas précis (dans le contexte spécifique du Web 2.0.) ?

Dans la mesure où les individus sont de plus en plus, eux-mêmes, générateurs de contenu et de données personnelles sur le Web 2.0, il conviendrait en effet d'aligner le régime de la Convention 108 sur le régime de la Directive 95/46/CE et de prévoir une exclusion des données traitées pour l'exercice d'activités exclusivement personnelles ou domestiques.

De plus, de façon pratique, il serait impossible pour les autorités de règlementer toutes les activités personnelles des individus (ex : carnets d'adresses, etc.).

Il conviendra cependant d'interpréter cette exclusion de façon prudente et de définir avec attention ce qui relève ou non d'une activité personnelle ou domestique. Cela est particulièrement tangible concernant les profils des internautes sur les réseaux sociaux. Cette question relève largement du pouvoir d'interprétation des autorités de protection des données. 3 A cet égard, des lignes directrices ont d'ores et déjà pu être dégagées par le Groupe de l'article 29, notamment dans un avis sur les réseaux sociaux.

5. La définition du traitement automatisé n'inclut pas la collecte des données : le fait que la collecte fasse l'objet d'une disposition spéciale est-il problématique ? Est-ce suffisant ? Doiton ajouter d'autres opérations à la liste existante ? La définition du maître de fichier devrait être revue : plusieurs critères doivent-ils être répertoriés, ces critères doivent-ils se cumuler, peut-il y avoir plusieurs maîtres de fichier pour un seul fichier?

Il conviendrait en effet d'avoir une définition de la notion de traitement qui soit la plus large possible, tant les opérations réalisées sur les données personnelles ont tendance à se multiplier et se diversifier.

Il serait ainsi approprié d'ajouter la notion de « collecte » des données. D'autres éléments pourraient également être ajoutés dans la définition de traitement, dont notamment la consultation, l'utilisation, etc.

La définition de la Directive 95/46 pourrait offrir une base de réflexion utile.

6. De nouvelles définitions sont peut-être nécessaires, comme celle du sous-traitant ou celle du fabricant des équipements techniques.

Il serait en effet souhaitable d'introduire dans la Convention 108 la définition du sous-traitant, et ce dans la mesure où, de façon croissante, le traitement effectif et quotidien des données personnelles se situe dans les mains du sous-traitant et non dans celles du responsable de traitement.

On constate notamment que les pratiques d'externalisation de certaines prestations impliquant des traitements de données deviennent la norme et il est d'autant plus impérieux d'encadrer de façon plus efficace le rôle du sous-traitant. A cet égard, une cohérence avec la définition de la Directive 95/46 précisant qu'il s'agit de l'organisme agissant « pour le compte » du responsable du traitement est nécessaire.

Plus encore, le régime de responsabilité du sous-traitant devrait être davantage harmonisé et encadré au niveau européen.

L'introduction de la définition du sous-traitant n'aurait toutefois véritablement de sens que s'il vient s'y rattacher des obligations ou des principes, à l'image de ce qui est prévu actuellement dans la convention au sujet du « maître de fichiers ».

Par ailleurs, il serait opportun d'encadrer une responsabilité des concepteurs et producteurs de technologies et des industriels. Cette approche favoriserait la mise en oeuvre du principe de « *privacy by design* » et permettrait de responsabiliser les concepteurs et producteurs de technologies quant aux produits qu'ils mettent en circulation sur le marché.

La promotion de labels et de procédures d'agrément pourrait également être encouragée.

Le rôle des opérateurs de réseaux et des fournisseurs d'équipements pourrait être évoqué plus avant.

Principes de protection

7. De nouveaux principes pourraient être ajoutés à la Convention, comme le principe de proportionnalité qui devrait s'appliquer à l'ensemble des opérations réalisées sur les données. Ce principe est également lié à celui de minimalisation des données qui vise à limiter la collecte des données à caractère personnel au strict minimum, voire à y mettre un terme lorsque cela est possible.

Il conviendrait de déterminer plus précisément le contenu d'un tel principe de proportionnalité. En effet, il existe d'ores et déjà à l'article 5 de la Convention précisant que les données personnelles

collectées ne doivent pas être excessives au regard des finalités poursuivies. La plus-value d'un principe spécifique de proportionnalité reste à préciser et à mettre en balance face au risque d'une multiplication, et partant d'une perte de lisibilité, des droits existants.

Par ailleurs, le principe de « limitation de la collecte des données » (« *data minimisation* »), bien qu'il ne soit pas expressément nommé, est déjà présent, dans une certaine mesure, dans l'article 5 de la Convention 108. L'étendue de ce principe mériterait ainsi d'être explicitée et mieux définie.

8. La question du consentement devrait-elle être envisagée en étroite liaison avec le principe de transparence et l'obligation d'informer, ou en tant que condition nécessaire à satisfaire un traitement loyal et licite avant toute autre action ?

Le consentement est en effet clairement lié à l'obligation d'informer la personne sur le traitement de ses données personnelles. L'obligation d'information de la personne participe de la réalisation d'un consentement libre et éclairé. Toutefois, le consentement doit en outre être une condition et offrir, dans certains cas, une base légitime pour le traitement des données.

A l'heure actuelle, les modalités de recueil du consentement sont loin d'être adéquates – par exemple le simple fait d'afficher des règles de confidentialité sur un site n'est pas suffisant pour en déduire qu'un consommateur a donné son consentement informé. Il est primordial de s'assurer que la mise en oeuvre en pratique du consentement est flexible et conviviale/facile d'utilisation (« user-friendly »).

Le consentement explicite pourrait être mis en oeuvre en pratique par le recueil du consentement préalable des personnes dit « opt-in ».

Il est ainsi fondamental de relativiser le rôle que peut jouer le consentement comme base légale pour le traitement. Il existe des hypothèses où le consentement n'offrira pas de base satisfaisante pour procéder à un traitement. Il en va ainsi notamment dans l'hypothèse du traitement des données d'un salarié par son employeur. Dans ce cas, le consentement ne pourra être considéré comme libre du fait du lien hiérarchique unissant le salarié à son employeur.

Il doit ainsi exister, à côté du consentement, d'autres bases pour procéder à un traitement, comme par exemple l'existence d'un lien contractuel, d'une obligation légale, etc.

Ces éléments pourraient être détaillés dans la Convention 108 et les articles 7 et 8 de la Directive 95/46/CE. Ils offrent des éléments de réflexion intéressants à cet égard.

Il serait par ailleurs utile d'intégrer dans la Convention 108 une définition du consentement précisant qu'il s'agit d'une manifestation de volonté libre, spécifique et informée.

La préparation d'un avis du G29 sur la notion de consentement pourrait là encore alimenter la réflexion du Conseil de l'Europe. Cet avis devrait tendre à décrire les règles de l'UE existantes dans le domaine et à proposer des modifications pour l'avenir. Cet avis pourrait être adopté en avril 2011.

9. La Convention 108 devrait-elle aborder la question de la légitimation des traitements de données comme le fait la Directive 95/46 dans son article 7 ? Faudrait-il dresser une liste de fondements légitimes pour le traitement des données ?

Au regard de la réponse ci-dessous, il apparaît en effet extrêmement utile d'aborder cette question de la légitimation des traitements de données. Cela devrait se faire sur la base de l'article 7 de la Directive 95/46/CE, mais également sur la base de l'article 8 relatif aux données sensibles.

Il serait à cet égard pertinent de dresser une liste des différentes bases légitimant le traitement. Une telle liste est, de plus, de nature à donner des lignes directrices aux individus, aux responsables de traitements, aux autorités de protection des données personnelles, etc.

10. La Convention 108 ne fait pas de référence expresse à la compatibilité nécessaire entre l'utilisation des données et le but initial de leur collecte. Or, aujourd'hui, les données à caractère personnel sont généralement utilisées à des fins qui vont bien au-delà de celles initialement prévues, d'où la question de la compatibilité

La question des traitements ultérieurs est, en effet, de plus en plus fréquente et devrait être traitée. Des précisions devraient être introduites notamment pour permettre les traitements ultérieurs à des fins historiques, statistiques ou scientifiques.

Il est également complexe en pratique de vérifier, au cas par cas, la compatibilité entre la finalité initialement envisagée et la finalité du traitement ultérieur.

11. La définition des catégories particulières de données faisant l'objet d'une protection accrue est très large, ce qui pourrait entraîner une application excessive de cette restriction : est-ce l'information ou son traitement qui est sensible ? Devrait-on ajouter d'autres catégories de données, comme les numéros d'identification (nationaux) et les données biologiques ou biométriques ?

Il serait opportun de prévoir un régime d'encadrement particulier (en France, il s'agit d'un contrôle préalable des autorités de protection des données au travers d'un régime d'autorisation) pour les données sensibles. Les conditions dans lesquelles il est possible de traiter ces données sensibles devraient être détaillées dans la Convention 108. Se limiter simplement à l'exigence de garanties appropriées définies par le droit national, comme c'est le cas actuellement dans la Convention, manque en effet de précision. Il conviendrait ainsi de 6 rappeler le principe de l'interdiction du traitement des données sensibles (dû à la nature des données) pour donner, dans un second temps, une liste d'exceptions (consentement, obligation légale, défense des intérêts vitaux de la personne, etc…). Les données doivent être sensibles par nature et non en raison de la finalité poursuivie.

Concernant l'ajout d'autres catégories de données sensibles, plusieurs propositions pourraient être envisagées :
- inclure les données génétiques
- inclure les données biométriques
- évoquer l'origine ethnique plutôt que l'origine raciale ou, tout au moins, affirmer que le Conseil de l'Europe rejette toutes théories tendant à déterminer l'existence de races humaines distinctes.
- ajouter une exemption pour les traitements statistiques et la recherche scientifique

Les données de géolocalisation et les données de trafic pourraient également faire l'objet d'un encadrement particulier.

Le G29 prépare actuellement un avis sur les données sensibles. Cet avis pourrait être adopté à la plénière qui se tiendra en avril 2011.

12. Une protection spécifique pourrait également être appliquée à certaines catégories de personnes sur lesquelles portent les données. Les enfants, en particulier, peuvent avoir besoin d'une protection spéciale en raison de leur vulnérabilité. Y-a-t-il un besoin de dispositions spécifiques à la protection des enfants ? Si tel est le cas, quels aspects devraient aborder ces dispositions ?

Des droits et des règles de protection spécifiques pour les mineurs semblent nécessaires, ces derniers n'étant pas à même d'exprimer seuls un consentement libre, spécifique et éclairé lors d'une collecte.

En fonction des finalités poursuivies, un meilleur encadrement de certains traitements (par exemple concernant la collecte des données personnelles à des fins commerciales) et l'interdiction d'autres traitements (par exemple dans le cadre du profilage) pourraient être envisagés.

Se pose également la question de l'absence d'harmonisation des critères de définition du « mineur » en Europe. Il serait peut-être préférable de tenir compte de la faculté de discernement de la personne concernée ou encore de sa faculté à exprimer son consentement.

De telles règles spécifiques pour les mineurs ne devraient pas nécessairement être contenues dans la Convention 108 mais pourraient être développées dans le cadre d'un instrument spécifique, comme une recommandation du Comité des ministres.

En droit français, il n'existe aucune disposition spécifique relative aux mineurs dans la loi de 1978. En pratique, la CNIL encourage ainsi tout responsable de traitement désireux de collecter les données personnelles de mineurs à : (1) obtenir le consentement préalable des parents et leur donner les moyens de s'opposer à la collecte et (2) fournir une information claire au mineur sur ses droits. Il convient également d'exiger une information adaptée et lisible pour le mineur.

Enfin, en pratique, il est nécessaire, pour les Etats et pour les autorités, de mettre en place des actions de sensibilisation à l'attention des jeunes sur les dangers inhérents aux nouvelles technologies.

13. L'article 7 de la Convention porte sur la sécurité des données au sens restrictif du terme, à savoir la protection contre la destruction accidentelle ou non autorisée, la perte accidentelle et l'accès non autorisé, la modification ou la diffusion. La notion de sécurité devrait-elle également inclure un droit pour les personnes concernées d'être informées des violations de la sécurité des données ?

Il serait effectivement souhaitable de mettre en place une obligation de notifier les failles de sécurité pour tous les responsables de traitement – aussi bien en ligne que hors ligne. Cette obligation permettrait incontestablement de réduire les risques en matière de sécurité.

Une réflexion est actuellement en cours au sein de l'Union européenne sur la généralisation d'une telle obligation de notifier les failles de sécurité.

Il conviendra cependant d'être attentif à bien définir le champ d'application de cette obligation de notification : convient-il de notifier aux autorités de protection des données ? aux individus victimes de ces failles ? qui serait soumis à cette obligation ?

La notification de faille de sécurité aux personnes concernées pourrait valablement être posée comme principe général. Mais une certaine latitude doit être laissée pour sa mise en

oeuvre, permettant notamment de définir des exceptions ou des délais justifiés ou l'absence manifeste de risque ou un intérêt public (enquête de police).

14. Il existe certains risques découlant de l'utilisation des données de trafic et de localisation (données techniques accompagnant une communication) car ces données peuvent révéler les mouvements, orientations, préférences et associations avec d'autres. Avons-nous besoin de règles particulières pour l'utilisation de ce type de données ?

Il serait opportun de prévoir un régime de protection renforcée pour les traitements visant à localiser les individus dans l'espace.

Une première option serait d'inclure les données de géolocalisation d'un individu dans les catégories de données « particulières » définies dans l'article 6 de la convention. Dans sa rédaction actuelle, cet article exige simplement que des garanties internes soient définies dans le droit interne.

Cependant, il faut être prudent à ne pas placer un frein à certaines innovations technologiques. En effet, de nombreuses technologies actuelles utilisent des données qui peuvent révéler indirectement la localisation géographique d'un individu comme, par exemple, le paiement par carte bancaire, la carte électronique de transport public ou les appels téléphoniques GSM. Ainsi, qualifier les « données de géolocalisation » comme données « sensibles » de manière générale pourrait être risqué.

Une deuxième option serait d'ajouter des éléments clairement distincts dans la Convention visant plus spécifiquement à imposer des garanties appropriées pour « les données à caractère personnel utilisées dans des traitements ayant pour finalité de révéler la position dans l'espace d'un individu », ce qui permettrait, d'une part, d'exclure les données qui peuvent révéler la localisation d'un individu mais dont ce n'est pas la finalité et, d'autre part, de ne pas nécessairement mettre les traitements de géolocalisation au même niveau que les données « spéciales » de l'article 6.

Une troisième option, proposée à la question 20 est de proposer un droit spécifique à ne pas être géolocalisé.

15. Faut-il mettre en place des systèmes de responsabilisation, ainsi qu'une obligation de prouver que des mesures efficaces ont été prises pour garantir le plein respect de la protection des données ?

Le principe d' « *accountability* » apparaît en effet comme un principe positif, qu'il convient d'encourager.
Il convient néanmoins d'être attentif dans la définition d'un tel principe. La CNIL estime que ce principe doit, de façon pédagogique, préciser l'obligation générale, pour les responsables de traitement, de prendre toutes les mesures appropriées pour mettre en oeuvre les principes relatifs à la protection des données. Plus encore, le responsable de traitement doit être en mesure de démontrer à l'autorité, à la demande de cette dernière, qu'il a pris ces mesures appropriées.

A cet égard, l'avis 3/2010 du G29 donne des indications utiles sur ce principe.

En aucun cas ce principe d' « *accountabity* » ne devrait se substituer aux obligations existantes et il doit nécessairement s'accompagner d'un contrôle *a posteriori* des autorités de protection des données.

Par ailleurs, le principe d' « *accountability* » pourrait se traduire en mesures concrètes, par exemple à travers la possibilité ou l'obligation, pour les responsables de traitement, de désigner des correspondants informatique et libertés. *16. Devrait-on appliquer le principe du « respect de la vie privée dès la conception » (Privacy by Design) qui vise à prendre en compte la question de la protection des données dès le stade de la conception d'un produit, d'un service ou d'un système d'information ?* Le principe de « *privacy by design* », neutre sur le plan technologique et applicable aussi bien aux responsables du traitement des données qu'aux concepteurs et producteurs de technologies, devrait être ajouté aux principes fondateurs de la Convention 108. Des référentiels devraient être développés par les autorités de protection des données et pourraient inclure le développement de bonnes pratiques et de standards, y compris le paramétrage par défaut, plus protecteur de la vie privée. Le développement et l'utilisation des technologies renforçant la protection de la vie privée pourraient être améliorés par la mise en place de labels, développés par les autorités de 9 protection des données. La loi française prévoit ainsi en son article 11 que la CNIL peut délivrer des labels.

Enfin, la mise en place d'évaluations d'impact sur la vie privée devrait être encouragée.

Droits – Obligations

17. Le droit d'accès ne devrait pas se limiter aux données mais devrait couvrir l'accès à l'origine des données, c'est-à-dire la personne qui est à l'origine de la communication. Ce droit devrait-il également couvrir l'accès à la logique du traitement ?

La personne concernée devrait en effet pouvoir obtenir les informations permettant de connaître et de contester la logique qui sous-tend le traitement en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.

Plus généralement, il est important d'améliorer les modalités, pour un individu, d'exercer son droit d'accès à ses données, en particulier dans le monde numérique. Il faut encourager le développement de l'exercice des droits d'accès, de rectification et d'opposition par voie électronique, notamment par Internet, dès lors que le responsable de traitement dispose d'un service de communication au public en ligne.

En toute hypothèse ? les modalités d'exercice du droit d'accès ne sont pas suffisamment détaillées dans la Convention 108. Il conviendrait notamment de reconnaître à la personne concernée le droit d'obtenir les informations relatives à l'origine des données ou aux flux transfrontières de données.

L'exercice du droit d'accès par les personnes concernées auprès des responsables de traitement, mais également leurs droits de s'opposer à la collecte, de corriger, effacer ou bloquer les données devraient être gratuits. La loi française prévoit que le droit d'opposition à la collecte à des fins de prospection doit se faire sans frais (Art.38) et que le responsable de traitement peut subordonner la délivrance d'une copie au paiement d'une somme ne pouvant excéder le coût de la reproduction (Art. 39.I), sauf en cas de demandes abusives, notamment par leur nombre, leur caractère répétitif ou systématique (Art. 39. II). De plus, pour l'exercice du droit de correction, la loi française prévoit que le responsable de traitement doit justifier, à la demande du demandeur et sans frais, qu'il a procédé aux opérations exigées (Art.40).

La Convention 108 prévoit que la personne concernée doit pouvoir obtenir, à des intervalles raisonnables et sans délais ou frais excessifs, la confirmation de l'existence ou non, dans le fichier automatisé de données à caractère personnel la concernant (la formulation pourrait par ailleurs être revue). De tels délais maximums ne sont toutefois pas prévus pour répondre

à l'obligation de rectifier ou de supprimer des données traitées en infraction à la protection des données.

18. Le droit d'opposition se justifie dans les cas où le traitement des données ne repose pas sur le consentement de la personne concernée. Le lien entre droit d'opposition et droit à l'oubli pourrait être examiné, ainsi que la possibilité de garantir le respect et l'exercice de ce droit.

Le droit d'opposition se justifie également quand le traitement repose sur le consentement. En application de la loi française, le droit d'opposition ne s'applique pas en revanche quand le traitement répond à une obligation légale ou lorsque ce droit a été écarté par une disposition expresse de l'acte autorisant le traitement.

Concernant le droit à l'oubli, ce dernier n'est pas seulement lié au droit d'opposition mais également à d'autres droits des personnes. Le concept de droit à l'oubli pourrait être introduit dans le cadre de la modernisation de la Convention 108. Ce principe devrait toutefois être défini de façon précise et pourrait couvrir notamment les principes existants de droit à la suppression des données, y compris par des tiers, ou encore la limitation dans la durée de conservation des données personnelles. Ce droit doit par ailleurs être concilié avec d'autres principes, tels que le devoir de mémoire, la liberté d'expression ou l'expression journalistique.

19. Devrait-il y avoir un droit qui garantisse la confidentialité et l'intégrité des systèmes d'information ?

Un droit à la confidentialité et l'intégrité des systèmes d'information semble très proche de l'obligation d'assurer la sécurité des données personnelles traitées. Il est notamment précisé, à l'article 7 de la Convention, que des mesures de sécurité appropriées doivent être prises pour empêcher la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisée.

La plus value d'un droit à la confidentialité et l'intégrité des systèmes d'information reste ainsi à préciser et à mettre en balance par rapport au risque de dilution et de perte de lisibilité des droits contenus dans la convention.

20. Faudrait-il introduire le droit de tout individu à « ne pas être localisé / tracé» (identification RFID) ?

Il pourrait être utile de réfléchir à l'opportunité d'introduire un droit à ne pas être localisé ou tracé. Un tel droit aurait notamment des vertus pédagogiques et de lisibilité pour les individus.

Un tel principe devrait s'accompagner de la nécessité de respecter l'ensemble des principes relatifs à la protection des données (qualité des données, sécurité, etc…) et devrait être assorti d'exceptions et de dérogations.

21. Les utilisateurs des technologies de l'information et de la communication devraient-ils avoir le droit de rester anonymes ?

Il convient tout d'abord de favoriser l'utilisation de procédés d'anonymisation ou de « pseudonymisation ».

Ces procédés favorisent la limitation, autant que possible, de la collecte des données personnelles. Par ailleurs, un statut distinct pourrait être défini pour les données pseudonymes, notamment pour trouver un statut intermédiaire entre les données anonymes, pour lesquelles 11 aucune protection ne s'applique, et les données personnelles impliquant l'application de toutes les règles informatique et libertés (notamment en termes de notifications, etc…).

La question d'un droit spécifique à rester anonyme mérite d'être étudiée. Il convient notamment d'examiner si un tel droit n'est pas d'ores et déjà couvert par d'autres principes de la Convention et s'il n'y a pas un risque de dilution des droits.

22. La Convention 108 devrait-elle aborder la question du juste équilibre entre la protection des données à caractère personnel et la liberté d'expression (nouveau concept de la presse et du journalisme dans le contexte du Web 2.0.) ?

Il est en effet important de trouver un juste équilibre entre protection des données personnelles et liberté d'expression.

Ainsi la loi de 1978 informatique et libertés comprend un chapitre XI sur le traitement des données aux fins de journalisme et prévoit ainsi un aménagement des règles existantes dans ce domaine, notamment sur la limitation de la durée de conservation des données, l'interdiction de collecter des données à caractère politique, le droit d'accès, les transferts, etc.

Des dispositions similaires pourraient être intégrées dans la Convention 108 afin de favoriser un équilibre entre protection des données et droit à l'information. Il serait notamment utile de préciser, au plan européen, les exemptions et dérogations dont les traitements peuvent bénéficier.

Cet équilibre doit toutefois également être réglé de façon casuistique par les autorités de protection des données et les tribunaux (et ce de la même manière que la Cour européenne des droits de l'homme établit un équilibre au cas par cas entre les articles 8 et 10 de la CEDH).

Sanctions et recours

23. Devrait-on introduire des recours collectifs dans la Convention ? Faut-il examiner l'introduction d'autres mécanismes de règlement des litiges ?

Du fait de la nature-même des litiges en matière de protection des données, souvent avec des sommes peu élevées en jeu et des dommages difficile à quantifier, les personnes concernées exercent rarement de recours.

Tout comme dans d'autres domaines du droit, il serait important que les personnes concernées puissent obtenir compensation. Une procédure de « recours collectif » permettrait aux personnes concernées ayant subi des dommages du fait du même responsable de traitement, par exemple suite à une faille de sécurité, d'aller ensemble devant les tribunaux réclamer réparation. La mise en place de cette procédure permettrait également d'inciter les entreprises à mieux respecter la loi.

Toutefois, les conséquences pratiques et l'impact potentiel sur les différents acteurs devraient être attentivement évalués avant de mettre en place des recours collectifs en Europe. 12 Par ailleurs, il conviendrait de donner la possibilité aux autorités de protection des données d'intervenir librement devant les juridictions judiciaires et administratives lors d'instances en cours.

Enfin, les mécanismes alternatifs de règlement des litiges devraient être favorisés. Toutefois, ces mécanismes alternatifs ne devraient jamais être une première étape obligatoire ou être le seul moyen de résolution des litiges à la disposition des personnes concernées.

Droit applicable en matière de protection des données

24. Doit-on envisager une règle qui déterminerait le droit applicable au traitement des données (dans les cas où différentes juridictions sont concernées) ?

Il est devenu aujourd'hui extrêmement complexe, à l'heure de la mondialisation des technologies et de la vie des affaires, de déterminer quelle loi relative à la protection des données personnelles va s'appliquer à un cas précis. Il y en effet un double risque : celui d'une lacune de protection (par l'absence de loi applicable) ou au contraire celui de l'application cumulative, de plusieurs droits à une même situation.

Cette difficulté est exacerbée par le fait que plus de deux tiers des Etats du monde n'ont pas de loi sur la protection des données ou d'autorité indépendante chargée d'en assurer le contrôle. Aussi il apparaît souhaitable de mieux coordonner et harmoniser, au niveau européen voire mondial, les règles de détermination du droit applicable.

Il pourrait ainsi être proposé d'intégrer dans la Convention 108 une disposition sur le droit applicable. Le critère principal pourrait être l'application du lieu d'établissement du responsable de traitement. A titre subsidiaire, la loi applicable serait celle du pays vers lequel le responsable de traitement dirige son activité de façon spécifique.

Ces critères devraient encore être affinés et l'avis du G29 sur le droit applicable, adopté en décembre 2010, fournit des indications utiles sur ce point, notamment dans sa conclusion sur la révision de la Directive 95/46/CE.

L'intégration d'une règle sur le droit applicable dans la Convention 108 serait ainsi particulièrement souhaitable, en particulier pour encadrer de façon plus cohérente l'activité d'entreprises multinationales. Toutefois, il est certain qu'une telle disposition pourrait donner lieu à d'importantes discussions voire même constituer un obstacle pour une éventuelle ratification de la Convention 108 par des Etats tiers au Conseil de l'Europe.

Le fait que la Convention pourrait comporter des dispositions d'effet direct milite cependant en faveur d'une disposition sur le droit national applicable.

Autorités de protection des données

25. Comment garantir leur indépendance et assurer une coopération internationale entre les autorités nationales ?

Il apparait nécessaire de renforcer les critères et les garanties d'indépendance des autorités de protection des données.

A cet égard, l'arrêt récent du 9 mars 2010 de la Cour européenne de justice de l'union européenne (CJUE), sur les autorités de protection des données des Länder allemands (affaire C-518/07), a permis de clarifier le concept de « complète indépendance ». Cette jurisprudence pourrait être reflétée de façon plus explicite dans la Directive mais également dans la Convention 108.

Il convient, dans le même temps, de laisser de la place à la variété des systèmes nationaux et de ne pas imposer de modèle unique.

Il conviendrait par ailleurs de prévoir, de façon plus explicite, des garanties d'indépendance financière pour les autorités de protection des données.
Ainsi, une obligation explicite à la charge des Etats membres de fournir des moyens suffisants pour les autorités de protection des données pourrait être incluse dans la Convention. La loi française prévoit ainsi que la CNIL « dispose des crédits nécessaires à l'accomplissement de ses missions » (article 12).

Concernant l'indépendance financière, une réflexion pourrait être engagée sur les modalités de financement des autorités, par exemple également par le biais de redevances perçues auprès des responsables de traitement. Mais une telle disposition semble trop spécifique et devrait être réglée en dehors du cadre général offert par la Convention 108.

Par ailleurs, concernant la coopération internationale entre autorités, il apparaitrait opportun, non pas d'imposer, mais de préciser et faciliter encore davantage la coopération entre les autorités lorsqu'elles sont confrontées à des infractions à la législation relative à la protection des données à caractère personnel, y compris dans le domaine police/justice.

La Convention pourrait aborder les conditions dans lesquelles les autorités (et non pas seulement les Etats) coopèrent entre elles afin de garantir le respect des lois de protection des données, voire même de définir les modalités/protocole pour mener des actions communes, notamment pour des plaintes internationales ou des contrôles transfrontières. Il conviendrait également de clarifier quels sont les pouvoirs d'action des autorités à l'étranger.

Dans le cadre de l'Union européenne, un avis spécifique est actuellement élaboré sur cette question et pourrait être adopté d'ici à la séance plénière du G29 du mois d'avril 2011.

26. Faut-il spécifier leur rôle et leurs missions ?

Il est essentiel que toutes les autorités nationales soient dotées d'une pluralité de moyens d'intervention, harmonisés « vers le haut » et renforcés, afin d'accomplir les missions qui leur sont confiées. Il convient tout particulièrement de renforcer leur pouvoir de contrôle *a posteriori*. Il s'agit également d'une condition nécessaire à une coopération entre autorités.

Flux transfrontières de données

27. La Convention 108 avait pour but de concilier la protection effective des données et la libre circulation de l'information sans considération de frontières. Ces principes ont été 14 *développés plus avant dans un protocole additionnel (STCE 181, 2001). En principe, un niveau de protection adéquat doit être assuré.*

28. Doit-on entièrement réexaminer la notion de « flux transfrontières de données » à l'heure d'Internet, où les données circulent instantanément à travers les frontières ? Serait-il utile de fixer des règles minimales internationalement reconnues pour garantir le respect de la vie privée sans considération des frontières ? Quel pourrait en être le contenu ?

Le régime de la Convention 108 et de son protocole additionnel relatif aux flux transfrontières de données pourrait être renforcé et adapté aux dernières évolutions technologiques, comme le *cloud computing*.

Pour ce qui est de la France, le régime juridique applicable est avant tout régi par les dispositions définies par la Directive 95/46/CE. Aussi, les instruments développés, dans le cadre de l'Union européenne, pour encadrer les transferts, sont dans l'ensemble satisfaisants. En revanche, concernant l'encadrement de ces flux transfrontières, il est nécessaire d'harmoniser au niveau européen et de simplifier les procédures nationales d'autorisation des transferts internationaux. Il est toutefois indispensable de conserver, dans le même temps, un haut niveau de protection des individus de façon à ce que les données personnelles ne soient pas transférées vers des pays ou des entreprises n'offrant pas une protection adéquate et suffisante.

Les règles relatives aux transferts contenues dans le protocole additionnel à la Convention 108 mériteraient ainsi d'être détaillées davantage et ce pour favoriser notamment une pleine harmonisation avec les règles contenues dans la Directive 95/46/CE.

Enfin, il est en effet devenu urgent de développer des standards mondiaux pour garantir la vie privée sans considération de frontières, et ce d'autant plus que plus des deux tiers des Etats du monde n'ont pas de loi sur la protection des données ou d'autorité indépendante de contrôle.

En définitive, il convient de soutenir pleinement les efforts engagés pour développer un instrument international dans le domaine de la protection des données. Ainsi, le processus des « standards internationaux », initié par la Conférence internationale des commissaires à la protection des données, est à soutenir sans réserve. Ce processus a débouché sur l'adoption d'une résolution à Madrid qui offre un corpus de principes communs, universellement acceptés. Il convient toutefois désormais de traduire cette avancée en une réalité juridique concrète. Les gouvernements doivent se saisir de cette question pour initier un projet de conférence intergouvernementale sur ce sujet. Le prochain G8, qui se tiendra en mai 2011 sous présidence française, pourrait être l'occasion de placer la nécessité de cet instrument international à l'agenda des pouvoirs publics.

La formulation de certains principes dans les standards internationaux, dans la mesure où ils ont été universellement acceptés, pourrait inspirer la rédaction de certaines principes de la Convention 108 (ex : sur le principe d'*accountability*, l'adoption de mesures proactives, etc…)

Surtout, il convient de soutenir également sans réserve le processus complémentaire visant à promouvoir la Convention 108 comme un instrument mondial relatif à la protection des données. La Convention 108 offre une base solide qui pourrait être ratifiée par des Etats non membres du Conseil de l'Europe.

29. Doit-il y avoir des règles différentes pour le secteur public et le secteur privé ? S'agissant notamment du secteur privé, doit-on avoir davantage recours à des règles d'entreprise contraignantes, éventuellement associées à un système de responsabilisation du destinataire final pour garantir le respect de ces règles ?

Il importe en effet de régir, de façon protectrice, les flux transfrontières de données personnelles, tant pour le secteur privé que pour le secteur public.

Les règles régissant les transferts internationaux sont, pour ce qui est des pays de l'Union européenne, d'ores et déjà définies par les règles de la Directive 95/46/CE, ainsi que par les dispositions des décisions-cadre 2006/960/JAI et 2008/977/JAI du Conseil pour ce qui concerne les échanges de données traitées dans le cadre de la coopération judiciaire et policière en matière pénale. Il convient notamment de réussir à articuler pleinement ces règles communautaires et celles de la Convention 108, notamment pour régir les transferts de pays membres de l'UE vers des pays non membres de l'UE mais ayant ratifié la Convention 108.

En ce qui concerne les données traitées à des fins commerciales, il convient ainsi en particulier d'encourager le recours aux règles internes d'entreprise pour réguler les flux transfrontières de données. Toutefois, un système de règles internes d'entreprises (ou BCR pour *Binding Corporate Rules*) a d'ores et déjà été développé dans le cadre de l'Union européenne. Ce système satisfaisant et efficace, permettant d'obtenir un haut niveau de protection à l'échelle de sociétés faisant partie d'un même groupe, doit être utilisé et promu plus avant.

Par ailleurs, les BCR pourraient être intégrés dans la Directive 95/46/CE à l'occasion de la prochaine révision de cet instrument. Il faut veiller à ne pas créer un système parallèle et divergent d'encadrement des transferts au sein du Conseil de l'Europe. Un tel système ferait « double emploi » (et double charge pour les entreprises) par rapport au dispositif existant dans le cadre de l'Union.

Il pourrait en revanche être utile d'initier une réflexion pour mettre en place un système de reconnaissance mutuelle des BCR dans des pays non membres de l'UE ayant ratifié la Convention 108 et offrant une protection adéquate. Une telle suggestion mérite toutefois plus ample réflexion.

Sous réserve également de la mise en place d'un mécanisme de suivi efficace et du renforcement de certaines de ses dispositions, la ratification de la Convention 108 pourrait jouer un rôle pour la reconnaissance de la protection adéquate par l'Union européenne.

S'agissant des données traitées par les autorités publiques, et en particulier les données traitées à des fins répressives, il apparaît nécessaire qu'un encadrement spécifique des flux transfrontières de données soit mis en place. En effet, au vu de la sensibilité des informations qui peuvent être traitées dans ce cadre, et des risques spécifiques pour les droits et libertés fondamentaux que de tels échanges comportent, notamment pour la protection de la vie privée des personnes concernées, il convient que des règles spécifiques soient prévues pour permettre de tels échanges de données, à l'instar de ce que prévoient les décisions-cadre adoptées par le Conseil de l'UE.

En particulier, la communication de données traitées par des autorités répressives à des autorités publiques d'un autre Etat partie, ou à des personnes privées, doit être subordonnée à la mise en place de mécanismes rigoureux de suivi de la mise en oeuvre de la Convention, afin de s'assurer que les Etats destinataires des données assurent un niveau de protection des données équivalent à celui assuré par l'Etat qui transmet les informations.

Rôle du comité consultatif

30. La Convention 108 a créé un comité chargé de faciliter son application et, le cas échéant, de l'améliorer. Doit-on renforcer le rôle jusqu'ici principalement consultatif du comité ? Si oui, quelles fonctions faut-il développer plus avant : l'activité normative, le règlement des litiges, le suivi ?

Le rôle du Comité consultatif de la Convention 108 est absolument essentiel dans l'architecture du travail du Conseil de l'Europe sur la protection des données.

Le Comité doit donc continuer à faciliter l'application de la Convention 108. En particulier, une des grandes réalisations de ce Comité a été de développer des projets de recommandations à l'attention du Comité des ministres sur des applications concrètes de la Convention 108. Il convient de saluer, entres autres, les recommandations sur la protection des données dans le cadre du profilage, de l'emploi, des assurances, de la police, etc.

Ces recommandations constituent autant de lignes directrices particulièrement utiles pour les gouvernements, les autorités de protection des données, les entreprises, les individus, etc.
Aussi, le rôle du Comité, en tant que Comité consultatif, est de délivrer une expertise et de formuler des propositions à l'attention des gouvernements au sein du Comité directeur sur la coopération juridique pour proposition au Comité des ministres.

Par conséquent, il serait extrêmement souhaitable de revoir la composition de ce Comité consultatif. Actuellement chaque Etat désigne son représentant, qui peut être un représentant du gouvernement (en général d'un ministère) ou un représentant d'une autorité de protection des données. Or il semble que ce sont bien les autorités de protection des données qui sont les premières en charge d'appliquer la Convention 108. Ce sont les autorités et non les gouvernements qui bénéficient de l'expérience et de l'expertise pratique dans le domaine de la protection des données.

Il conviendrait donc de modifier la Convention 108 pour préciser que le Comité consultatif est composé des représentants des autorités de protection des données des pays ayant ratifié la Convention. Ce Comité consultatif ferait ensuite des propositions au comité directeur de coopération juridique, composé uniquement de représentants des gouvernements.

Ce comité directeur de coopération juridique ferait, à son tour, des propositions au Comité des ministres, représentant là encore les Etats.

Une telle modification du Comité consultatif de la Convention permettrait de bénéficier pleinement de l'expertise des autorités de protection des données et permettrait de ménager tant une représentation des autorités que des gouvernements.

Cela correspond d'ailleurs largement à la logique développée dans le cadre de l'Union européenne, avec la mise en place d'un Groupe de l'Article 29 composé d'autorités et du Comité de l'Article 31 composé des gouvernements.

Enfin, il n'est plus à démontrer que l'expertise des autorités est extrêmement souhaitée, notamment par les entreprises, dans la mesure où elle permet de dégager des lignes directrices et d'harmoniser les positions nationales adoptées par chaque autorité. Et ce sont en effet les autorités de protection des données, et non les gouvernements, qui sont, au premier chef, chargées du contrôle du respect, par les entreprises, des législations nationales se fondant sur la Convention 108.

Concernant ensuite la question du renforcement du rôle du Comité consultatif, il serait souhaitable de s'orienter vers un rôle de suivi renforcé. Il est en effet crucial de déterminer la manière dont est mise en oeuvre la Convention 108 au niveau national et de disposer de moyens d'action en cas de mauvaise mise en oeuvre.

CENTRE FOR SOCIO-LEGAL STUDIES

About Us:
We are a group of academics coming together under the umbrella of DP@CSLS, a research strand within Oxford University's Centre for Socio-Legal Studies (CSLS) concerned with data protection, privacy and the regulation of information. Further information on this initiative is available at http://www.csls.ox.ac.uk/dataprotection and on http://www.twitter.com/oxondataprotect. Although not all of us are associated formally with the Centre, we have all been involved in DP@CSLS activities. However, the views presented in this submission are solely personal, as opposed to organizational, in nature. This submission was written by Dr. David Erdos, principal investigator of the Leverhulme Trust funded Data Protection and the Open Society (DPOS) project. It was then reviewed and endorsed by the other members of the DP@CSLS Study Group.[247] *These other members are:*

- *Liam Curren, Researcher in Law & Solicitor, HeLEX Centre for Health, Law and Emerging Technologies, University of Oxford*
- *Richard Danbury, Barrister & D.Phil candidate, Faculty of Law, University of Oxford*
- *Noriswadi Ismail, Ph.D. candidate, Centre for Commercial Law Studies, Queen Mary University of London*
- *Dr. Nadja Kanellopoulou, Researcher in Law, HeLEX Centre for Health, Law and Emerging Technologies, University of Oxford*
- *Professor Lawrence Lustgarten, Emeritus Professor of Law, University of Southampton & Associate Fellow, Centre for Socio-Legal Studies, University of Oxford*
- *Steven McCarty-Snead, D.Phil candidate, Centre for Socio-Legal Studies, University of Oxford*
- *Nabiha Syed, MSt. student, Centre for Socio-Legal Studies, University of Oxford*
- *Asma Vranaki, D.Phil candidate, Centre for Socio-Legal Studies, University of Oxford*

[247] It is based on an earlier submission which a similarly constituted DP@CSLS Study Group made to the European Commission's consultation on "A Comprehensive Approach on Personal Data in the European Union" (January 2011).

Executive Summary

- *With the proliferation of increasingly intrusive mechanisms* via which information of a personal nature is being processed, ensuring an appropriately framed and enforced Data Protection (DP) law has never been more important.
- The Council's questions helpfully identify a large number of issues which should be addressed in order for data protection to respond to the challenges of the Web 2.0 context.
- Nevertheless, we are concerned that this reform process might ignore the need to reflect on the fundamental purpose of DP more closely which, in turn, is essential to determining its future shape and substance. There is also a danger of overlooking the need to carry out more work to, firstly, reconcile DP and other fundamental values and, relatedly, to respond to legitimate concerns of data controllers in regard to both normative and pragmatic problems with current law. The DP@CSLS Study Group puts forward a number of general proposals regarding these issues.
- The tension between DP and freedom of expression/information in the area of academic investigations constitutes a particular area which has problematically been ignored in the current reform process and in which the DP@CSLS Study Group has particular expertise. The DP regime has had a draconian and disproportionate effect on the activities of many researchers. There is a vital need to ensure that academics benefit on a fair and equal basis from the freedom of expression/information exceptions available to producers of other material for the public, such as journalists.
- Further difficulties concerning freedom of expression and DP arise, firstly, due to the highly divergent and in some cases very restrictive manner in which Data Protection interacts with freedom of expression in many countries which are signatories of Convention 108. This issue is becoming ever more pressing due in the context of the proliferation of citizen publishing and social networking. Although far from always enforced by national authorities, current DP law has the potential to illegitimately curtail freedom of expression, especially in new social media. Nevertheless, it may constitute an incoherent response to provide for a new blanket and total exemption from DP norms for all processing merely because it was 'non-commercial' and conducted by a single individual. To the contrary, this dilemma suggests the need to establish a broad special provision which reconciles on a principled basis the values of DP, including privacy, and freedom of expression/information as well as takes into account the size and structure of the data controller.

Section One: Introduction

Since its negotiation in 1981, the Council of Europe's Convention 108 has played a path-breaking role in shaping policy on DP and privacy not only within Europe but also worldwide. The importance of this law is only likely to grow as increasingly complex and invasive mechanisms for processing information of personal nature proliferate. At the same time, however, this law has faced many criticisms and challenges which have grown over time. Notably, within the UK context, in 2008, the then Information Commissioner Richard Thomas described the law as prescriptive, bureaucratic and "no longer fit for purpose".[248] The Council of Europe's questionnaire helpfully identifies numerous issues which must be addressed if Data Protection is to become more coherent and respond effectively to new technological challenges.[249] Nevertheless, we are concerned that the reform process may fail to appropriately address the following core issues:

- The fundamental or ultimate purpose of DP,
- Normative and pragmatic problems of compliance with this law,
- The need to reconcile DP and other values, notably freedom of expression and information.

It is impossible to highlight all issues of relevant concern under these headings in a single submission. Nor is it possible to frame a theoretically superlative framework for governing information of a personal nature. The DP@CSLS Study Group has therefore concentrated on suggesting practical solutions to those issues which have been particularly under-recognized so far and in which it has particular expertise. These are:

- The tension between DP and free flow of information and ideas in the academic (and particularly social) research area,
- The need to reconcile DP and freedom of expression in the context of the new social media.

The following parts of this submission are structured into two general and two more specific sections. Section two addresses the pressing and general need to resolve the fundamental purpose and scope of DP. Section three concentrates on the specific and neglected effect of DP on academic investigations and suggests how this effect could be resolved. Section four turns to the general tension between DP and freedom of expression especially in the context of new social media. Section five responds to a range of other normative and pragmatic problems identified by data controllers and others under the current Convention and then it putts forward suggestions for ameliorating those problems.

[248] Nicholas Timmins, "Data laws branded out of date", *Financial Times*, 8 July 2008.

[249] http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf.

Section Two: Determining the Purpose and Scope of Data Protection

The Study Group is concerned that despite nearly thirty years since Convention 108 was drafted, the basic purposes and nature of this body of law remains unclear and contested. Within the European Union, the Lisbon Treaty has now defined Data Protection as part of the fabric of fundamental human rights. In sum, the Charter states:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent agency.[250]

This wording, even more than Convention 108 itself, implies that DP should have a comprehensive scope, broad purpose and, given that it regards something fundamental, should seemingly be applied in a strict manner by the legal and regulatory authorities. More specifically, this position further implies that:

- The DP framework should apply not only to commercial and governmental operations but also in the areas of civil society, journalism, research and even at individual level.[251]
- The purpose of DP should encompass i) guarding against intrusions of fundamental privacy, ii) ensuring individual control over personal information in which an individual has a legitimate interest and iii) ensuring against the misuse of personal information when making decisions about a living individual.
- There should be clear and significant sanctions and remedies for DP violations, and enforcement through both public (regulatory) and private (individual) action.

Each of these understandings is highly contestable, however, in a wider context both within EU Member States and beyond. Writing back in 1986, Anne Morddel perceptively noted:

> [S]urveys and guidelines have led to data protection in most European countries, but it should be noted that the definitions of privacy, freedom of information, the right to information, and of information itself, have been clarified in no case. Because of this, of the data protection found in Europe, any one of the issues may appear as the primary concern of the law.[252]

[250] Article 8, Charter of Fundamental Rights of the European Union.

[251] At least where such processing moved beyond operations necessary for purely intimate personal activities (e.g. keeping a personal address book) and had the clear potential to violate other persons rights and interests (e.g. "publishing data to an indeterminate number of persons").

[252] Anne Morddel, "Background to the Data Protection Act," *Bulletin of the Records Management Society* 14 (1986): 5. In terms of her empirics, Morddel actually overstated the spread of DP legislation which, in fact, had only been adopted by a minority of Western countries in 1986. The lack of mass proliferation of DP legislation was a major

Despite transnational instruments including not only Convention 108 but also the EU Directive bringing certain levels of harmonization, divergences remain acute even within the EU. For example:

- "Pragmatic" regulators such as the UK's Information Commissioner's Office may favour largely confining the law to policing the use of personal data in discrete commercial and government operations. In terms of their focus on commercial operations, they would undoubtedly be supported by the approach of the United States Federal Trade Commission and APEC. Both these entities tend to see DP as a relatively narrow matter of consumer protection as opposed to an issue of fundamental human rights.
- Especially after their 2004 review of the law, it is clear that Sweden has a strong desire to narrow the focus of DP away from comprehensive control and privacy which remain important in many other European countries. A significant step down this road was made as a result of their 2007 amendments to the law which removed the need for most "unstructured" electronic data processing to comply with many DP norms. Whether these amendments are actually compatible with the Sweden's EU data protection responsibilities remains highly debatable. Nevertheless, there is a strong sense that, whilst unique in carrying through such amendments through a formal change in the law, Swedish understandings are mirrored at a practical level in a number of other approaches even within the EU.
- Despite the rhetoric of fundamental human rights, the actual implementation of DP in Convention 108 states remains extremely limited. This is a finding that is endorsed by both supporters and opponents of its basic structure.[253]

The interests of harmonization clearly require that these fundamental divergences should be addressed and a greater degree of commonness of purpose achieved. Especially given its recent entrenchment in the EU's Lisbon Treaty, it may well be that the core of the current dominant pan-European understanding (comprehensiveness of scope, breadth of purpose and relatively strict enforcement) constitutes the clearest achievable focal point for the future. Moreover, if appropriately implemented, such an understanding may have the advantage of encouraging the development of a coherent and common law of personal information privacy across different sectors of society. Nevertheless, such an ambitious understanding is not without significant pitfalls. In particular, in view of the massively different contexts in which such law seeks to regulate information of a personal nature[254], it is imperative that:

---

reason behind the European Commission's decision to push for what became the European Data Protection Directive in 1995.

[253] Lucas Bergkamp, "The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy," *Computer Law & Security Report* 18, no. 1 (2002), Yves Poullet, "The Directive 95/46/EC: Ten Years After," *Computer Law & Security Report* 22 (2006)..

[254] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, California: Stanford University Press, 2010), 238.

- The law explicitly and systematically balances and reconciles conflicting values both within DP (e.g. between privacy and ensuring the transparency of data processing operations) and, more significantly, between DP and other fundamental rights and interests, including, most notably, freedom of expression, association and information.[255]
- That the law be drafted in a flexible manner to allow for the crafting of appropriate special provisions and exemptions that respond to genuine concerns of data controllers about disproportionate and impracticable duties and responsibilities.

Unfortunately, current DP law has been criticized for significant failures in relation to these essential requirements. The following sections of this submission concentrate on examining these problems and proposing practical solutions both in relation to specific topics - DP and Academic Research (section three) and DP and the General Right to Freedom of Expression (section four) - and also in relation to more general contested matters in the current debate.

[255] This is partially recognized in the Green Paper when it states that "other relevant fundamental rights enshrined in the Charter, and the other objectives in the Treaties, have to be fully taken into account while ensuring the fundamental right to the protection of personal data." European Commission. "A Comprehensive Approach on Personal Data Protection in the European Union.".

Section Three: Data Protection and Academic Investigation

One important area where it has been cogently argued that Europe's current data protection has failed to get the balance right between conflicting values concerns *academic investigation*. DP law has had a serious effect on the conduct of academic investigation (otherwise known as research), with many arguing that it inappropriately restricts these activities. For example, medical researchers have argued that DP law has created unreasonable barriers to the obtaining and continued processing of essential data as well as serious legal tangles over the meaning of anonymisation. [256] This is said to lead to unacceptable selection bias in the data that can eventually be analyzed and, at the extreme, to even a complete inability to carry out pressing research in this area.[257] In 2004, a top UK cancer expert, Sir Richard Doll, announced that the framework was "utterly destructive" and that he would rather "go to jail for science" than comply with these and related rules.[258] In the same year, a trenchant *British Medical Journal* Editorial starkly stated:

> The deaths that will now occur because of the effects [of data protection] on British medical research attract less publicity than child murders; but the pointless obstacles that bone fide researchers, particularly epidemiologists, face when they seek access to individual medical records are now causing serious damage.[259]

Ordinary DP norms pose even more fundamental problems for academic investigations into social - including historical and political- affairs. These investigations are often necessarily fluid, norm-challenging, sometimes covert, individual and even identifiable. However, the interpretation of current DP law, at least in the UK, generally holds that such activities must comply with these standards.[260] This has also prompted concerns within the profession that are also beginning to appear in print.[261] The following commentary discusses key issues in this area.

---

[256] G-G Westrin and T Nilstun, "The Ethics of Data Utilisation: A Comparison between Epidemiology and Journalism," *British Medical Journal* 308 (1994). Judith Strobl, Emma Cave, and Tom Walley, "Data Protection Legislation: Interpretation and Barriers to Research," *British Medical Journal* 321 (2000). Amy Iversen et al., "Consent, Confidentiality, and the Data Protection Act," *British Medical Journal* 332 (2006).

[257] *Ibid*.

[258] Anna Fazackerley, "Top Cancer Expert, 91: "I'll Go to Jail for Science"," *Times Higher Education*, 27.02. 2004.

[259] Julian Peto, Olivia Fletcher, and Clare Gilham, "Data Protection, Informed Consent, and Research," *British Medical Journal* 328 (2004).

[260] Such an understanding is reflected in the data protection registration template drawn up by ICO for Universities (and the registration returns of the vast majority of the same), the official Data Protection Data of Practice for Higher Education and statements by authoritative interpreters of the Act including Carey and Jay. See Information Commissioner's Office, "N887 - University," https://www.ico.gov.uk/onlinenotification/PurposeDetails.aspx?key=ajq161&tid=377. (accessed 12 December 2010) Andrew Charlesworth. "Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998." (2008), http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/DPACodeofpractice.pdf. Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, 3rd Edition ed. (Oxford: Oxford University Press, 2009), 173. Rosemary Jay, *Data Protection Law and Practice* (London: Sweet and Maxwell, 2007), 537.

[261] Anne Barlow, "New Ethical Challenges for Socio-Legal Researchers: Slsa One-Day Conference," *Socio-Legal Newsletter*, no. 44 (2004). Odette Parry and Natasha S. Mauthner, "Whose Data Are They Anyway? Practical, Legal and Ethical Issues in Archiving Qualitative Research Data," *Sociology* 38, no. 1 (2004), Eric Barendt, *Academic Freedom and the Law: A Comparative Study* (Oxford: Hart Publishingd, 2010). David Erdos, "Stuck in the Thicket? Social Research under the First Data Protection Principle", (forthcoming 2011, *International Journal of Law and Information Technology*). David Erdos, "Lost in the Labyrinth? Social Research and the Data Protection Framework," (forthcoming 2011*, Information Communications and Technology Law*).

3.1 – Academic Social Research:
Problems:

It is difficult to overstate the degree of tension between many types of social research and a number of European DP provisions. Particularly problematic are (i) the rules regarding the provision of fair information to data subjects based on Article 8 of the Convention, (ii) restrictions on the processing of sensitive personal data based Article 6 of the Convention and (iii) a strict interpretation of the ban on transferring data to areas where data protection standards are deemed "inadequate". Turning to the first of these issues, data protection experts such as Rosemary Jay have specifically held that United Kingdom DP law makes *covert research* "almost certainly" illegal.[262] Meanwhile, analyzing law from across the European Union, Rosier and Vereecken state that "the researcher must, at a minimum, describe the main object of the research, *e.g.* a study on the causes of failure at school or a study on the evolution of women's position at work".[263] As Canadian scholar Kevin Haggerty has noted, the inability to resort to non-transparent methodologies can have profound and deleterious consequences for knowledge production:

> The requirement to be "up front" about the focus of your research can simply preclude valuable forms of critical inquiry. Researchers, for example, who wanted to accompany and interview police officers at work in order to learn about police racism (or corruption, sexism, excessive use of force, etc.) would likely see their research grind to a halt at the first sign of a consent form informing officers of the research topic. The same is true for a host of other critical scholarship that might seek to investigate high-profile, contentious issues involving powerful people or agencies.[264]

Moreover, it should be stressed that covert research has proved essential to the gathering of necessary data which serves a strong public interest.[265] Even greater restrictions are placed on any investigation which uses sensitive personal data. As such data are defined broadly and categorically within current DP law including Article 6, many social investigations will involve the processing of sensitive personal data.[266] However, the restrictions implemented in relation to this in many signatories to the Convention can be extremely severe at least when handling data that the data subject neither manifestly placed into the public domain nor expressly and explicitly consented to their processing. For example, in the UK (by no means the least restrictive jurisdiction within the EU) such processing is only allowable if it:

(a) is in the substantial public interest;
(b) is necessary for research purposes;
(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and

---

[262] Anne Barlow, "New Ethical Challenges for Socio-Legal Researchers: SLSA One-Day Conference," *Socio-Legal Newsletter*, no. 44 (2004). A similar analysis of the law is provided by Karen Rosier and Isabelle Vereecken, "Data Protection Aspects within the Framework of Socio-Economic Research"(Brighton: Insitute for Employment Studies (2003)), http://www.respectproject.org/data/415data.pdf (accessed 12 December 2010).

[263] Rosier and Vereecken, "Data Protection Aspects within the Framework of Socio-Economic Research".

[264] Kevin Haggerty, "Ethics Creep: Governing Social Science Research in the Name of Ethics," *Qualitative Sociology* 27, no. 4 (2004): 406.

[265] Simon Holdaway, "'An inside Job': A Case Study of Covert Research on the Police," in *Social Research Ethics: An Examination of the Merits of Covert Participant Observation*, ed. Martin Bulmer (London: Macmillan, 1982), Nigel Fielding, "Observational Research on the National Front," in *Social Research Ethics: An Examination of the Merits of Covert Participant Observation*, ed. Martin Bulmer (London: Macmillan, 1982), Don Sapatkin, "Was This Ethical? Scientists Dare to Decieve," *The Philadelphia Inquirer*, 24.05.2010.

[266] Great Britain Economic and Social Research Council, *Research Ethics Framework*, 8.

(d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.[267]

Whilst of considerable value to most routine social research, the strict and peremptory nature of these criteria is completely inappropriate for the needs of contemporary historical and critical socio-political studies. These projects often publish information in non-anonymous form and this (or even other related processing) may both cause certain persons damage or distress or lead to a measure or decision being taken in relation to them. Whilst such results should be studiously avoided where they are unwarranted, what is striking is that this formulation prevents such action even when it is manifestly justified. Writing on similar provisions included in the United States Common Rule for the Protection of Human Subjects in Research,[268] Linda Shopes outlines the difficulties:

> [F]or historians, a deep disjunction exists between the Common Rule's concern for privacy and the canons of historical inquiry. At times information in an interview, if made public, can indeed place a person at risk of criminal or civil liability, or be damaging to his financial standing, employability, or reputation. Yet historians' deepest responsibility is to follow the evidence where it leads, to discern and make sense of the past in all its complexity; not necessarily to protect individuals from their past actions.[269]

She further identifies the critical problem with such doctrinaire prohibitions:

> What is at issue is the notion of critical inquiry, inquiry that does challenge, that may be adversarial, that may even "expose," as interviews with Klansmen and women and with Nazi collaborators, for example, have done. Yet current regulations, interpreted narrowly, can have a chilling effect on historian's freedom to pursue difficult topics. Moreover, historians pursuing research on some twentieth-century topics may find that they have acquired critical, if controversial information with profound consequences for public life; they may further determine that the public's need to know may have greater urgency than may be allowed for in current regulations.[270]

At the extreme, the specific rules governing the processing of sensitive personal data for research could even prevent a candid inquiry into genocide if this might lead to measure or decision being taken in relation, or damage or distress caused, to a genocide perpetrator. Finally, the ban of exporting data outside the EEA absence "adequate protection" (from which there is no Research exemption) has led to the drawing up of policies which, if interpreted literally, would make the worldwide publication of any personal data in academic investigation illegal absent explicit consent. Thus, the UK's Economic and Social Research Council argues that:

> Data may not be collected from, or transferred to countries outside the EEA unless that country has adequate data protection regulations, or the explicit consent of the data subject has been obtained, or there is an appropriate contract with the recipient of the data, specifying appropriate data protection requirements that must be upheld. In most cases, the only safe option will be to ensure that participants give explicit consent for overseas transfer during data collection.[271]

Meanwhile, the University of Newcastle states not only that "[p]osting data on the Internet automatically discloses it on a worldwide basis"[272] but also that, under the data export

---

[267] Data Protection (Processing of Sensitive Personal Data etc.) Order, 2000, para 9.

[268] 45 C.F.R. pt. 46 (2009).

[269] Linda Shopes, "Oral History, Human Subjects and Institutional Review Boards", http://www.oralhistory.org/do-oral-history/oral-history-and-irb-review/ (accessed 12 December 2010).

[270] ———, "Institutional Review Boards Have a Chilling Effect on Oral History" (2000) http://www.historians.org/perspectives/issues/2000/0009/0009vie1.cfm (accessed 12 December 2010).

[271] Economic and Social Research Council. "Framework for Research Ethics." (2010), http://www.esrcsocietytoday.ac.uk/ESRCInfoCentre/Images/Framework%20for%20Research%20Ethics%202010_tcm6-35811.pdf.

[272] University of Newcastle. "Data Protection Staff Handbook Faqs Data on the Internet.", http://www.ncl.ac.uk/data.protection/handbook27.htm.

principle, "data cannot be transferred electronically to the greater part of the world, including Russia and Eastern Europe, USA, Canada, South America, Africa, Middle East, Asia, China, Australia or New Zealand".[273] In practice, these regulations have resulted in social investigators attached to academic institutions being especially and uniquely restricted in terms of what activities they may carry out. This practice has resulted in a diminution of academic freedom. Perhaps even more importantly, it has resulted in the loss of important forms of knowledge production. This damages society as a whole for, as British sociologist Robert Dingwall notes, "[i]f what has traditionally been the most disinterested source of information, the universities becomes systematically handicapped…all citizens lose out".[274]

Solutions

Much like other social investigations by non-academic writers and journalists, academic social researchers gather, process and then disseminate their findings to the public often in literary form. As Haggerty notes:

> Both social scientists and journalists conduct interviews, videotape people and events, undertake forms of participant observation, and, in recent years, have increasingly scrutinized online discussion groups. Media outlets also produce a host of quantitative knowledges through their own in-house research units or contracts with private research firms. Newspaper and magazine surveys of university students are prominent examples of such media generated statistical studies. Television broadcasters routinely conduct opinion polls, and Web surveys are now an omnipresent volume of research on pressing social issues.[275]

It is a violation of legal equality to treat agents who are essentially engaged in the "same enterprise"[276] in this divergent manner. This is especially the case as, compared to the low-grade "infotainment" output of a considerable portion of the Press, academic investigation is generally internally "disciplined by a professional ethic and a regulative ideal of truth-telling".[277] European Convention jurisprudence under Article 10 concerning the right to "receive and impart information and ideas without interference" generally holds that expression of high value to society should be especially protected. However, mainstream interpretations of European DP law turn this logic on its head. There is a strong case that, even under the existing scheme, social research should be regarded as a form of literary processing which should benefit from the same as that provided for journalism (and artistic purposes). **For the future, what is absolutely essential is that:**

- **the new Convention includes specific provisions for freedom of expression and makes crystal clear that academic social investigation must be able to benefit from the this provision on an equal basis to other public expressive activities.[278]**

This would be in line with other OECD jurisdictions, such as Japan, which explicitly exclude both journalism and academic investigation from the need to comply with general DP norms.[279]

---

[273] ———, "Data Protection Staff Handbook - Eighth - Transfer of Data," http://www.ncl.ac.uk/data.protection/handbook17.htm.

[274] Robert Dingwall, "The Ethical Case against Ethical Regulation of Humanities and Social Science Research," *21st Century Society* 3, no. 1 (2008): 3.

[275] Haggerty, *supra* note 16 at 395.

[276] Dingwall, *supra* note 26 at 54

[277] Dingwall, "The Ethical Case against Ethical Regulation of Humanities and Social Science Research," 6.

[278] David Erdos, "Freedom of Expression Turned on Its Head? Academic Inquiry, Journalism and the Data Protection Framework," (2011) (manuscript available on request).

[279] Section 50 (3), *Act on the Protection of Personal Information*.

3.2 – Non-social academic research especially in the medical sphere

The general Research provisions of most European DP member states are much better suited to the governance of non-social, and especially medical, academic research. In sum, they are based on an understanding that such highly important social activities require extensive use of personal data in order to flourish and, furthermore, that individuals do not have a legitimate interest in a high level of data protection (as traditionally conceived) so long as three stipulations are upheld:

- Non-particularity: That data is "not processed to support measures or decisions with respect to particular individuals"[280]
- Non-malfeasance: That no "substantial damage or substantial distress is, or is likely to be, caused to any data subject".[281]
- Security: That all appropriate steps are taken to ensure against any unauthorized or unlawful processing which would undermine the two substantive conditions above.[282]

Difficulties are created by the considerable confusion around exactly in what way, and to what extent, the law provides an exemption from ordinary DP provisions where research complies with the above conditions. Several of the current problems are the result of a general tightening of the law in this area (notably in the UK context, from the pre-Directive *Data Protection Act* 1984[283] to the post-Directive *Data Protection Act* 1998) coupled with extremely risk-averse action by a number of institutions (such as certain Health Authorities) when faced with a confusing legal situation. Further problem areas are created by the difficulty of determining what "anonymized" means in this context.[284] In sum, we suggest that the following clarifications be made:

- That if such academic research makes use of data obtained indirectly from the data subject (e.g. using medical notes) then if the three conditions above are complied with it should be presumed, absent overriding reasons to the contrary, that an exemption from providing an information notice to data subjects applies.
- That if data are collected directly from the data subject but are being used tangentially for academic research in compliance with the three conditions, no requirement for the routine provision of an information notice to research subjects should extend beyond giving an indication that such data will be used for "research purposes".

---

[280] Section 33 (5), *Data Protection Act* (1998) (UK).

[281] Section 33 (1) (b), *Data Protection Act* (1998) (UK).

[282] Schedule 1, Paragraph 7, *Data Protection Act* (1998) (UK).

[283] Paragraph 7 (a) of Schedule 1 of the UK *Data Protection Act* 1984 provided that "[w]here personal data are held for historical, statistical or research purposes and not used in such a way that damage or distress is, or is likely to be caused, to any data subjects the information in the data shall not regarded for the purposes of the first principle [on fair and lawful obtaining and processing] as obtained unfairly by reason only that its use for any such purpose was not disclosed when it was obtained".

[284] In *Common Services Agency v. Scottish Information Commissioner* [2008] UKHL 47 (2008), the UK House of Lords ruled that, if a Data Controller holding de-identified data also held manually "other information" which could in principle link the de-identified data back to individuals, then the de-identified data alone would constitute not just personal data but also sensitive personal data. This was apparently the case even if the Controller had no intention of making such a link.

- That if academic research takes place in full compliance with the above conditions, it may be carried out without the consent of the data subject in DP terms, and, moreover, that absent very serious overriding reasons to the contrary, data subjects will not be able to stop such processing as a result of raising an objection.

Section Four: Data Protection and General Public Freedom of Expression

4.1 - Problems

The manner in which DP interacts with freedom of expression constitutes one of the most difficult and pressing issues confronting policy in this area. The explanatory memorandum of Convention 108 indicates that Article 9 (exemptions and restrictions) may be relied upon in order to safeguard freedom of the Press.[285] However, the Press is far from the only entity with a fundamental interest in public freedom of expression. In fact such interests are shared not only by other long-standing social actors such as academic researchers but, in fact, by every human being. The need to ensure legal protection for legitimate public freedom of expression, whilst balancing this where appropriate with the rights and interests which DP aims to protect, is become ever more pressing with the growth of blogs, social networking sites and citizen journalism. Unfortunately, current DP law within Convention 108 states shows major flaws in this area. For example, within the EU which is governed by the more specific journalism, literature and art provisions provided for in Article 9 of the EU Directive, the following problems have been identified:

- The Article has been transposed into Member State law in wildly divergent ways. In some countries no formal exemption for public expression is provided at all whilst in others journalistic, artistic and literary expression benefit from a virtually complete exemption from ordinary DP requirements. Finally, in yet other countries, domestic DP law provides fairly wide exemption from many DP requirements whilst holding such controllers to certain other disproportionate duties such a requirement to register journalistic, artistic or literary processing operations with the national regulator.[286]
- The Article only provides an exemption for those public activities which are solely journalistic, artistic or literary. Although this is broader than protection only for the Press, it is still too narrow. For example, it has been held to exclude both speech from socio-political actors and activities which take place on social networking sites. For example, in the case of *Quinton v. Pierce* (2009), the England and Wales High Court held that a politician's expression to the public through an electoral leaflet could not benefit from the journalistic, artistic or literary provisions. In the context of the massive expansion of the "new social media" such restrictions are becoming more and more pressing. This also increasingly possesses the potential to interfere other fundamental rights, namely, those of freedom of association and assembly.
- At the same time the increasingly invasive ways in which personal information is being handled publicly suggests that such activities should not generally be absolutely exempt from the values which DP seeks to protect, but that a principled balancing should prevail.

[285] We do note that whilst only the Press is explicitly mentioned, the Convention does not rule out the use of Article 9 in order to safeguard wider interest in freedom of expression. Given this, we would Convention 108 signatories to make wider exemptions than has traditionally been the norm within DP laws.

[286] This situation applies, for example, under the current UK data protection scheme. See Mike Holderness, "Data Protection Required," *Freelance: Newsletter of the London Freelance Branch, NUJ* (2008).

4.2 - Solutions

The problems with the current implementation Convention 108 in terms of its interaction with public freedom of expression suggests than any modified Convention should instantiate the following:

- **A new clause should be drafted which explicitly entreats signatories to provide a balance between the fundamental interest in freedom of public expression and the values which DP seeks to protect and, furthermore, state that this indicates the need for wide-ranging, but not absolute, exemptions from ordinary DP rules for such activities. The possibility of expressing some of the core minimum of such exemptions, in conformity with Article 10 of the European Convention, needs to be explored.**
- **The new explanatory memorandum should explicitly state that this provision protecting public freedom of expression is not only applicable to the Press. In principle, this exemption should hold the potential to apply to any public expression; however, this does underscore the need for this exemption to be qualified in nature and subject to the aforementioned balancing scheme.**

Particular problems exist in relation to the spread of public processing of personal data by individual persons for non-commercial reasons. As the Council of Europe's questionnaire points out, even thought a number of signatories may provide complete exemption for certain forms of domestic processing, Convention 108 itself does not exclude such processing from its scope. Within the EU context, exclusively domestic processing is excluded from the scope of the Data Protection Directive.[287] However, this excludes data which is disclosed to an "indeterminate number of persons".[288] Publishing data live on the internet, which has become a hallmark of many forms of processing by individuals in the Web 2.0 era, is obviously the *sine qua non* of disclosure to an indeterminate number. For the future, it may be suggested that the best solution would simply be to draft a domestic purposes exemption which extends even to activities which disclose data to an indeterminate number. However, this "solution" has significant problems attached to it. Firstly, it appears that, especially with the growth of the open data movement, many of the most invasive and unjustifiable ways in which personal data may be processed are increasingly carried out by natural persons for non-commercial reasons. Moreover, the complete nature of the domestic purposes exemption indicates that it was designed primarily for those situations where individuals did not exert significant power as a result of their handling of personal information. This is patently not always the case in the internet age.[289] Secondly, such a complete exemption would hide the need to come up with a principled reconciliation between values. It would also lead to anomalies. For example, would such an exemption be lost when a number of people began cooperating, albeit on a non-commercial basis, in the disclosure of data to an indeterminate number of persons? If so, how would such a cut-off be determined and on what coherent basis? These problems indicate

[287] Information Commissioner's Office, "Response to the Ministry of Justice's Call for Evidence on the Current Data Protection Legislative Framework," http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Notices/response_to_moj_dpframework.ashx.

[288] Council and Commission Common Position Statement for Entry in the Minutes (1995) confirmed by ECJ in *Lindqvist* (2003).

[289] See Information Commissioner's Office, "Response to the Ministry of Justice's Call for Evidence on the Current Data Protection Legislative Framework."

that a better solution would be to, firstly, ensure that such individual activities can benefit fully from a new and broader freedom of public expression provision and, secondly, only impose any other data controller responsibilities on individuals in a clearly defined and proportionate manner. In relation to the latter issue, this would probably involve developing a hybrid system of regulation in relation to social networking sites (e.g. providing users who face a complaint with the option of having such issues resolved by the owner of the social networking site and only if such procedures are manifestly inadequate providing a recourse to more formalized measures) and providing a full exemption for such controllers from some of the more onerous DP responsibilities (e.g. subject access). Of course, these activities would still be subject to other applicable laws, the highlighting of which could further ensure a more principled approach to regulation.

Section Five: General Suggestions Regarding the Future of European Data Protection

It is clearly beyond the scope of this submission to provide a comprehensive analysis of how European DP law should be rectified. However, in closing we put forward a range of suggestions to expand on the over-arching understanding of submission as regards the ways in which European DP law should develop. The general contours of this understanding were laid out in section two of this submission. In summary, we believe that a comprehensive and broad DP law in Europe needs to:

- Be flexible and able to be fully reconciled with other fundamental values and also the legitimate pragmatic concerns of data controllers and data subjects alike.
- Reduce the "thicket" of laws which have ended up reducing legal certainty, and preventing a principled understanding of data protection amongst the public.
- Lessen bureaucratic and formalistic burdens on most data processing operations so as to free up resources to focus on reasonable areas of concern.
- Provide real and effective protection against the serious and unjustifiable types of data processing which continue to proliferate.

It is this broad perspective that grounds our necessarily rather cursory analysis of the range of issues outlined below.

5.1 – The concept of "personal data"

Although we recognize that European DP law is based on a notion of comprehensive coverage, we are concerned that the range of information covered by the term "personal data" is unreasonably broad. In sum, the Convention 108 defines personal data as literally any information relating to an identified or identifiable person (Article 2). It is impossible to overstate the potential breadth of this definition. For example, when the Library Association and others drew up information for the library community in the early 1980s in relation to this, they held, after seeking guidance from the Data Protection Registrar (now the ICO), that generally:

> The question of whether the data are "public" or "private", however these terms may be defined, has no bearing [on this]…this is a matter of law, not common sense, and failure to comply with the requirements of the Act [then the *Data Protection Act* 1984] attracts penalties.

More specifically they held that even a combination of author and a title of one of their publications would be personal data about that person. Furthermore they stated:

> It is probable that ISBNs would be considered to be personal identifiers. Titles associated with a living individual, such as the Queen, the Archbishop of Canterbury, the Dalai Lama or the Duke of Wellington are also considered to be identification data within the meaning of the Act.[290]

Even broad theorists of privacy such as Daniel Solove have argued that such understandings of what sort of information of an identifiable nature should be regulated are overly broad. For example, he states that such definitions are:

> [T]oo broad because there is a significant amount of information identifiable to use that we do not deem as private. For example, the fact that a person is a well-known politician is identifiable to her….[Such a] definition provides no reasonable limitation in scope.[291]

[290] Data Protection Working Party Joint Consultative Committee, *Data Protection Guidelines for Library, Information and Related Services* ([London]: Aslib, 1985), 2/1-3/1.

[291] Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven; London: Yale University Press, 2007), 25.

Given that "political opinion" is deemed "sensitive personal data" it is even the case that the processing of certain clearly non-private data (such as the names and political affiliations of politicians) will constitute not just the processing of "personal data" but even the processing of "sensitive personal data".[292] In 2003, Lord Justice Auld in the England and Wales Court of Appeal sought to address these problems when he ruled that an individual's information should only be considered personal if it is "information that affects his privacy, whether in his personal or family life, business or professional capacity".[293] Whilst we appreciate that this formulation is not without its problems, it is unfortunate that this contribution resulted in a strong backlash especially elsewhere in the EU. [294] In sum, **we think it essential that in the future personal data does not cover such information, the processing of which does not, nor is likely to, significantly interfere with the values of privacy, fairness and non-discrimination that DP law was designed to protect.** At a minimum, this exclusion would apply to a wide range of publicly available data as well as certain non-public but relatively innocuous data concerning a person's professional, as opposed to truly private, life (e.g. professional contact details etc.).

5.2 – The future of notification

The bureaucratic and formulistic burden of current DP law is very clearly highlighted in the requirement across many Convention 108 signatories that almost all forms of data processing be notified with the national data protection authority and that these details, including the name and address of the data controller and designees (itself a potential invasion of privacy), then be placed on a public register. Whilst in an age before the mass use of the internet, such universal requirements may have been of some value, we believe this requirement is now completely disproportionate and, in fact, serves no useful purpose. As the RAND report from 2009 stated:

> Registers of data controllers were seen as only useful to lawyers conducting due diligence exercises. It was noted that consumers did not seem to be consulting the registers, either because they were unaware of them, or because they were unable to use the information in the registers to determine whether or not their own data was being processing.[295]

We therefore recommend that, as in the case of other OCED countries such as Australia, Canada and New Zealand, Convention 108 signatories be urged to reform their law so that it does not have any such notification requirements. Even if notification is not entirely abolished, we stress separately that processing under the purposes of freedom of public expression must be specifically and totally exempt from this duty. **This is particularly important as such requirements currently conflict with the general, albeit not indefeasible, right to anonymous electronic communication.[296]** Of course, in all cases it will still be necessary for the national data protection authority (and where necessary the courts) to have the power in appropriate cases to require data controllers (if necessary even on criminal penalty) to provide them with certain details of their processing operations including their name and address. Such powers, however, should and will only need to be exercised for a particular reason and in a proportionate manner.

---

[292] Information Commissioner's Office, "The Exemption for Personal Information," (Wilmslow, Cheshire: Information Commissioner's Office, 2008).

[293] *Durant v. Financial Services Authority* [2003] EWCA Civ 1746.

[294] This reaction culminated in the publication of a report by the Working Party which substantially reiterated the previously broad definition. See European Commission Article 29 Working Party on Data Protection. "Opinion 4/2007 on the Concept of Personal Data." (2007), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[295] Neil Robinson et al. "Review of the European Data Protection Directive." (RAND, 2009), http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf.

[296] Holderness, "Data Protection Required."

5.3 – The need for a principled approach

More generally, we would like to stress that the general law of DP must be based on broad principles. Unfortunately, the current regime in many signatory states is stuck between a recognition of the importance of a principled approach and a number of provisions which reflect a belief that a general code for data processing can be drawn up for fair data use that is covering a wide, in fact near universal, range of activities. When questioned in Parliament about some of the code-like aspects of the proposed data protection law in 1998, the then Solicitor-General Lord Falconer responded for the UK Government:

> [T]he Data Protection Bill aims to lay down a detailed code. It must do so under the terms of the directive…On the other hand, the Human Rights Bill intends to lay down general principles.[297]

Such a hybrid approach to regulation that emphasizes both principles and a litany of specific, rigid, legally binding rules can increase legal uncertainty whilst not improving the coherent protection of the values that DP aims to protect. We also stress that in any discussion on the future of Convention 108 there needs to be greater discussion and clarity about the meaning and scope of **Article 9** (exemptions and restrictions). **We would generally stress the need for the law to allow for appropriate accommodation of the many competing legitimate interests which often arise in a number of areas, whilst ensuring that there is an appropriate protection for some of the core values and interests which the ordinary DP protects.**

5.4 – Sensitive Data and Data Controller-Data Processor Relations

The concept of "sensitive personal data" is currently defined categorically within the Article 6 of Convention 108. It includes any data consisting of information as to data subjects' racial origin, political opinion, religious or other beliefs, physical or mental health and condition, commission or alleged commission of an offence and criminal proceedings.[298] Especially given the breadth of the definition of "personal data", it is clearly necessary and important to ensure that more sensitive data is protected to a much higher level than is the case with other data which still might be considered personal. However, a major problem with this approach from the point of view of the data subject is that it may tend to limit enhanced protection under DP law to certain specific categories of data instead of taking a more principled approach. A major problem from the data controller's point of view is that the categorical approach has the severe potential of including within its reach information that is relatively innocuous. Thus, courts in the UK have tended to rule that all colour photographs including identifiable persons constitute "sensitive personal data" since they reveal information about the person's racial origin.[299] Another problem concerns the generally highly restrictive conditions in many Convention 108 States that need to be satisfied if any processing of sensitive personal data is to take place in many, when it has not been explicitly consented to by the data subject nor manifestly made public by them.[300] This suggests the following solutions:

- **That the definition of sensitive personal data instantiate a categorical approach but with a proviso that, even if falling within these categories, personal data will not be considered sensitive if the specific types of data in question are not generally likely to pose a particularly serious threat to the values of privacy, fairness or non-discrimination which DP law seeks to protect.**

[297] House of Lords, *Debates*, 2 February 1998, Col. 477.

[298] DPA, § 2.

[299] Campbell v. MGN Ltd [2002] EMLR 30. *Murray v. Big Pictures* [2008] EWHC 1908 (Ch).

[300] This latter condition of "manifestly being made public by the data subject themselves" is potentially broad but extremely opaque.

- **That Convention 108 states reformulate their law such that, at a minimum, all sensitive data processing which can be justified as being in the "substantial public interest" is lawful.**

5.6 – The question of subject access and freedom of private communications

The provisions implementing Article 8 of the Convention as regards concerning subject access are widely experienced as unduly burdensome by data controllers. It is important to understand that these provisions were originally drafted mainly as a mechanism for ensuring that data subjects could verify that their legitimate DP interests were not being disregarded in data processing.[301] In practice, however, they are now treated as an end in themselves. Two major problems present themselves. Firstly, responses to such requests can exert a disproportionate resource burden on data controllers. Secondly, especially as interpreted by many data controllers, this right interferes in some circumstances with the right to private correspondence which is also recognized as a fundamental right within European law.[302] This latter issue links to broader restrictions on such communications as a result of the rules on data processing (e.g. restricting the processing of any sensitive personal data). Thus, to take one example within the UK academic sector, the University of Birmingham email's policy in relation to data protection states that:

> **All** staff and students must…regard all email exchanges as "postcards", accessible to all…. On reception of an appropriate request, **all** emails must be disclosed to the person about whom they are written….Deletion of an e-mail is not sufficient. E-mails remain on the University server for 30 days post deletion. It is an offence to delete an e-mail after receipt of a request for disclosure.

The policy also states that no derogatory material about another should appear in any emails and that any such material will lead to "disciplinary action within the University against the writer".[303]

Potential solutions to these two problems are two-fold:

- **Firstly, alongside Article 10 of the Convention, a explicit provision should be included stated that DP law must be explicitly reconciled with the freedom of private communications. This would involve appropriate exemptions from general DP provisions (e.g. governing the processing of sensitive data as well as the export of data) as well as certain exemptions from the right to subject access which may also go further than generally provided for. It should be specifically investigated whether the 2007 amendments to Swedish data protection law provide an appropriate model for other Convention 108 signatories in this regard.**
- **The need to provide a limit to the right to subject access on resource grounds should be similarly investigated. Again, whether the 2007 amendments to Swedish data protection law provide an appropriate model should be specifically investigated.**

5.7 – The need for effective enforcement

[301] United Kingdom Government Home Office, *Data Protection Act: A Report on Structure* (London: HMSO, 1990).

[302] Article 8 (1), European Convention on Human Rights.

[303] University of Birmingham, "Guidance on Email in Relation to Data Protection," http://www.as.bham.ac.uk/legislation/docs/GUIDE_E-mail_Data_Protection.pdf.

Nothing written in this submission should be read as implying that we do not believe that there is a need for tough legal action against certain uses of personal data in particular situations. We are aware that, especially given technological developments, the potential for serious misuse of personal data is increasing every day. One of the main problems with current DP law is that it has not proved effective enough in responding to obviously illegitimate and damaging data processing activities. These limitations in effectiveness may be exacerbated by the generally extremely broad official remit of this law. It is certainly also the result of the generally low level of awareness and enforcement of this body of law. For an extreme example, the UK Information Commissioner's Office Annual Track for 2010 found that no more than 2% of private data controllers were aware of any data subject right included within the data protection scheme other than subject access. Perhaps most worryingly, this survey also showed clear evidence of a decline, as opposed to increase, in such awareness over time.[304] If a reformulated DP law is going to genuinely protect legitimate rights and interests, then it is absolutely essential that these problems are squarely addressed. In sum, following on the broader understanding that we have mapped out above, we recommend and endorse the following solutions:

- **The low level of private enforcement of DP norms should be investigated with a view to develop modifications aimed at increasing the level of such enforcement. In general, we envisage that the principled approach highlighted throughout this submission can 'free up' the law and increase its accessibility by leading to greater public understanding which also might also increase private enforcement. Additional modifications to improve private enforcement may include:**
    - **Providing relatively low-cost procedures for bringing such claims;**
    - **Providing remedies that encompass compensation for distress (as well as financial and other loss) whilst ensuring that such damages are set at a reasonable level that does not impose undue burden on data controllers;**
    - **Publicizing the availability of such procedures and remedies.**
- **Data protection authorities must play a greater role in creating awareness of DP law and fundamental DP norms, including amongst newly emerging data controllers who are often structured relatively loosely and generally have little awareness of DP compliance. Such authorities need to be more effectively resourced and to have a clearer commitment to a coherent and principled implementation of DP norms.**

[304] Social and Market Strategic Research. "Report of the Findings of the Information Commissioner's Office Annual Track 2010." (Social and Market Strategic Research, 2010), http://www.ico.gov.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_organisations.ashx.

Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Submission to the Council of Europe

Consultation on the Council's Discussion Paper

'Modernisation of Convention 108'

Nigel Waters, Research Fellow[1] and Professor Graham Greenleaf[2]

Cyberspace Law & Policy Centre
University of New South Wales (UNSW) Faculty of Law

March 2011

http://www.cyberlawcentre.org/

nigelwaters@pacificprivacy.com.au

+61 (2) 4981 0828

[1] Nigel Waters was principal researcher on the *Interpreting Privacy Principles Project, funded by the Australian Research Council, 2006-2010.* Nigel is also Principal of Pacific Privacy Consulting (www.pacificprivacy.org.au). He was Deputy Australian Federal Privacy Commissioner 1989-1997, and Assistant UK Data Protection Registrar 1984-89. He holds Masters degrees from the Universities of Cambridge and Pennsylvania and from the University of Technology, Sydney. Nigel is a Board member of the Australian Privacy Foundation (www.privacy.org.au) and represents Privacy International (www.privacyinternational.org) at privacy related meetings of international bodies including APEC and the OECD.

[2] Professor Graham Greenleaf has a research-only appointment as Professor of Law & Information Systems at UNSW Faculty of Law. He has a number of visiting international positions in Edinburgh, Seoul and Hyderabad. He is also Co-Director of the Australasian Legal Information Institute (AustLII) and associated international projects (particularly AsianLII, CommonLII & WorldLII). He was Chief Investigator on the *Interpreting Privacy Principles Project*. In 2011 he is completing a book on information privacy (data protection) laws in Asia and will be based in Europe from July-December.

MODERNISATION OF CONVENTION 108

Submission, March 2011, by Nigel Waters & Graham Greenleaf, Cyberspace Law & Policy Centre, University of New South Wales, Australia

Structured around questions posed in Consultation document

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

Submission: The Convention should remain a simple, concise and technology neutral instrument, while at the same time recognising and addressing some new characteristics of the present and future technological environment, in ways which we explain below.

2. Should Convention 108 give a definition of the **right to data protection** and **privacy**?

Submission: No - It would not be helpful to try to define the right to privacy in a data protection Convention – it is a set of interests which manifest themselves in different ways in different contexts, and sometimes need to be balanced against other interests. It is more appropriate to express them as a set of broad principles. There are other instruments such as the European Convention on Human Rights, and the case law interpreting it, where broad statements of privacy protection are appropriate, and different mechanisms used for enforcement.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Submission: Yes – it is important that the Convention and its principles apply broadly – any areas in which derogations from some principles may be justified need to be specific and focussed.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely **personal or household activity.** Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

Submission: This is a difficult issue – full application of privacy principles to the behaviour of private individuals would be onerous and oppressive – threatening other important freedoms and rights. But modern technology increasingly allows individuals to threaten the privacy of others in ways that were previously only available to organisations, and some controls and restrictions are therefore justified. One approach to handling this difficult issue is by the broad statements of privacy protection in the ECHR and similar human rights instruments, at the international level. Some consideration could be given to making the privacy protections in those instruments more specific. At the national level, the issue can partly be addressed by statutorily defined rights of privacy where interpretation by the Courts has a major role, although cost and other barriers to access to courts is a significant problem. Low cost tribunals may have an important role to play.

5. The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

Submission: The only principle currently applying to collection is in Article 5 - that Personal data undergoing automatic processing shall be: (expressly, in (a)) "obtained and processed fairly and lawfully", and (implicitly) that data collected should be "adequate, relevant and not excessive ..." (in (c)) and "accurate" (in (d)). We submit that it would be helpful to include 'collection' in the definition of automatic processing so that all of the principles apply, where relevant, to collection. The principle needs to be strengthened by inclusion of a specific requirement that collection should not be excessive, and perhaps that it should not be by intrusive means. However, the 'data minimisation principle' (see response to Q8) is another way to achieve at least the first objective.

The definition of the **controller** of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?

Submission: The definition is satisfactory, criteria are and should be independent and there can be several controllers for one file.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Submission: These new definitions would only be necessary if provisions were inserted referring expressly to these entities. This may be necessary if provisions concerning 'privacy by design' are included, because it is essential that such a principle should apply to those designing technical equipment and not merely those utilising it, as it may be too late to factor in (or retro-fit) appropriate privacy protections once technologies are built without them. (see response to Q16)

See also response to Questions 14 and 20 below concerning the definition of 'personal data'.

Protection principles

7. New principles could be added to the Convention, such as the **proportionality** principle, which should apply to all operations carried out on the data. Such a principle is also linked to the **data minimisation principle** which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Submission: These are both significant principles which could valuably be added, and we strongly support their inclusion.

8. Should the question of **consent** be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Submission: The concept of consent is fraught with difficulty in a data protection context. If it is used it needs to be expressly defined as meaning free, informed and revocable, and not bundled with other consents. There are many current transactions which misleadingly use 'consent' when they in reality amount only to 'notice, and acknowledgement that nominated uses/disclosures are a condition of the transaction'. There should be a general principle that where genuine consent is a realistic option, it should be the preferred basis of fair processing (subject to other public interest exceptions), consistent with the overall aim of transparency in transactions involving personal data. This would be consistent with the introduction of a ' right of opposition' (see Q18) – a right to opt-out of secondary uses is necessary to avoid data controllers making them a condition of service.

It is important that any consent provision also expressly addresses the form in which consent is sought and recorded. The relevant provisions of the Canadian private sector privacy law (PPIPEDA) are relevant, as it the following proposed amendment to PPIPEDA: "the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting."

9. Should the **legitimate processing** be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

Submission: No – fair and lawful (i.e. not unlawful), coupled with other general principles of proportionality, data minimisation and non-intrusive collection, are appropriate criteria – a list of positive grounds for processing would inevitably be incomplete.

10. Convention 108 does not expressly mention **compatibility in relation to purpose**. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Submission: Compatibility is a subjective concept, and would be better expressed as 'uses or disclosures which are within the reasonable expectations of the data subject (to which a 'reasonable person' test would be applied). However, it should be made explicit that 'reasonable expectations' can only encompass uses or disclosures which a reasonable person would consider to be both fair and compatible with the original purpose of collection.

Uses and disclosures outside 'reasonable expectations' should only be permitted with (genuine) consent or under a prescribed exception.

11. **Special categories of data** which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

Submission: Unless the Convention is to specify the additional measures then there is limited value in defining 'special categories' or 'sensitive data'. Sensitivity is in any case subjective and contextual, and any list is likely to be arbitrary and incomplete. The proposed introduction of proportionality and data minimisation principles (see Q7) could replace the need for a 'special category' provision. The Convention should, however, explicitly accept the rights of member states to provide a higher level of protection for data which provides a higher level of risk to privacy interests than other personal data, proportional to that higher risk.

12. A specific protection could also be applied to certain categories of data subjects. In particular, **children** may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

Submission: There is no need for specific protections for certain categories of data subject. The proposed introduction of proportionality and data minimisation principles (see Q7) should adequately address the concerns about children and other potentially vulnerable groups. The explanatory materials accompanying the Convention could make this clear.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Submission: Yes, but not necessarily as part of a security principle – a right for data subjects to be informed of data breaches affecting them that meet specified threshold criteria should stand alone as a separate principle.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Submission: There would be no need for separate principles or rules for traffic or location data if personal data is defined as expressly including any information which enables or facilitates communication with a person on an individualised basis, whether or not it meets the current definition of personal data. This would include information about an individual's communications or location, and would include IP addresses, email address, other communications addresses, and geolocation data. (See also response to Q20 for additional inclusion of 'behaviour' in the definition)

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Submission: Yes – there should be an obligation to demonstrate that measures have been taken to ensure full respect for data protection rules. Caution should be taken in the use of 'accountability' which has been suggested in recent data protection debates as an alternative to specific requirements for compliance with rules. In particular, 'Accountability' cannot be and must not become an alternative to data export restrictions.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Submission: Yes, privacy by design should be expressly encouraged, although it may be difficult to operationalise this as a specific rule. A specific requirement to conduct privacy impact assessment (PIA) for major projects could help encourage privacy by design, but supervisory authorities need to be cautious about endorsing projects in advance in case it compromises their ability to subsequently investigate and enforce compliance.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

Submission: The right of access should include a right to be informed, on request, of the source of the data, also all recipients of the data (more specific than the general description given in collection notices), and also, where practicable, an explanation of the logic of the processing, e.g. credit scores.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

Submission: A right of opposition in the sense used in the EU Directive (Article 14); i.e. a right to opt out of processing, should be included, even when consent was originally granted, if it is reasonable for consent to be revocable in the circumstances.

A right to oblivion (to be forgotten) needs further consideration, as there may be many circumstances in which it is unreasonable or impractical, and even conflict with other principles such as security or data integrity, or interfere with the audit trail needed for accountability.

A 'right to be forgotten' should at the very least encompass a requirement that personal data should be deleted or made inaccessible once the purpose for its collection is complete, though this does not meet all situations where such a right is needed or justifiable.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

Submission: There can be no absolute guarantee of confidentiality or integrity – only that 'reasonable measures' be taken. Supervisory authorities do however need to be much stricter in their enforcement of these principles.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

Submission: There is no need for a separate 'right not to be tracked', if personal data is defined as expressly including information about an individual's communications, location or behaviour (See response to Q14)

21. Should everyone have a right to remain anonymous when using information and communication technologies?

Submission: An absolute right to anonymity is unreasonable and impracticable in many circumstances. Consideration should be given to inclusion of a principle similar to that already included in Australian privacy law as the 'anonymity prnciple'. Suggested wording:

> *"Individuals must have the option of not identifying themselves when dealing with an entity, or of using a pseudonym, except where there is either a legal requirement for identification or where it is impracticable for the entity to deal with individuals who have not identified themselves or who use a pseudonym."*

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

Submission: It is not appropriate for the Convention itself to try to balance every aspect of these interests, but some recognition of the public interest in freedom of expression would be desirable. This would be particularly relevant if the scope of the Convention was extended to cover individuals as data controllers (see Q4)(i.e. to cover activities such as citizen journalism).

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

Submission: The Convention does not currently expressly provide for complaints about breaches of the principles/rules – only for remedies where requests for correction etc are denied (Article 8(d)) (check Optional Protocol?). If the Convention is to include a requirement for complaint or ADR mechanisms, then it would be appropriate for it to expressly recognise the value of representative complaints (class actions).

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Submission: There may be more than one applicable law – both general and sectoral data protection laws and other laws with privacy related provisions. Insofar as data protection laws are concerned, it would be of value if, in relation to likely areas of conflict of laws, the Convention did state a choice of law rule, provided this was made subject to strong cross-border transfer rules (see Q27).

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

Submission: Supervisory authorities are only provided for expressly in the 2001 additional protocol to the Convention (CETS 181), and these provisions could usefully be incorporated in the Convention itself (see response to Q26 below). Clause 3 of Article 1 of the Protocol mandates independence, while Clause 5 requires international co-operation. It is probably not appropriate for the Convention to try to specify how these requirements are to be met.

26. Should their role and tasks be specified?

Submission: Article 1 of the Additional Protocol (CETS 181, 2001) specifies roles and functions of supervisory authorities. This should be incorporated in the Convention itself.
One particular task of a supervisory authority that needs to be spelled out is the obligation to account for their performance of their complaint investigation obligations, including by reporting to the public, on objectively determined criteria, of cases investigated (anonymised to the extent necessary to protect privacy but not otherwise), and by statistics including statistics concerning outcomes and remedies. Supervisory authorities must be able to demonstrate that they deliver remedies to complainants, otherwise their existence can simply be a cover for expanded surveillance activities.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

Submission: It remains appropriate to require an adequate level of protection as a condition of cross-border transfer. Member states of the Convention should require that the personal data concerning their citizens is protected if it leaves their jurisdiction. The provisions of the additional protocol should be moved inside the Convention.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

Submission: 'Globalisation' of 'minimum rules' is not desirable at all. It would simply be a 'race to the bottom' which would destroy any value in cross-border privacy protection. The Convention should establish the standard of protection it requires for citizens of member states, and adhere to that.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

Submission: The same basic principle of cross border transfer conditions should apply equally to the public and private sectors.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

Submission: We are not familiar with the operations of the consultative committee and have no particular opinion on this question.

CYPRUS - COMMISSIONER FOR PERSONAL DATA PROTECTION

Answers:

1. Convention 108 has proved to be a valuable tool that withstood the test of time against technological developments for the past thirty years. The modernization of Convention 108 should retain its technologically neutral character in order to withstand the new challenges.

2. Giving a definition of the right to data protection and privacy runs the risk of limiting the concept of privacy within the given definitions.

3. Yes, the modernization scheme should not result to a lesser level of protection than the one currently provided for by Convention 108. This concept is also in line with the comprehensive approach to data protection under the Lisbon Treaty and the horizontal application of data protection rules across the former pillars.

4. We are of the opinion that data processed by natural persons in the course of personal or household activities should be excluded from the scope of Convention 108.

5(a). We believe that the "collection" of data should be included in the definition of "automatic processing". We should explore the possibility of broadening the current list of operations.
(b). The definition of the "controller" should provide a list of cumulative criteria. The concept of several controllers for one file may cause some confusion, particularly as regards enforcement and the exercise of rights.

6(a). Yes, the definition of "processor" should be included.
(b) If the modernization of Convention 108 wishes to address/ tackle/ introduce the issue of "privacy by design", then the definition of the "manufacturer of technical equipment" should be included. (see also answer to q.16)

7. The proportionality principle should apply to all operations carried out on the data including collection (see answer 5(a)).

8. We believe that the principle of transparency should stand on its own. Consent is one but not the only condition for safeguarding transparency. The obligation to inform is a precondition for applying the principle of transparency. Therefore we believe that consent should be considered as a necessary condition to a fair and lawful processing among other conditions.

9. In spite of the fact that Convention 108 had been a general and broad legal instrument which enabled its parties to provide extended interpretations, it was used as a bench mark upon which Directive 95/46/EC was built. We believe that the modernization of the Convention should maintain its general character and it should not include a list of legitimate grounds for data processing, as laid down in Article 7 of the Directive, which may result to a more restrictive interpretation.

10. We agree that today's context should be revised to include the principle of compatibility in order to ensure that processing should not be incompatible with the initial purpose of the collection.

11. (a) We are of the opinion that the primary object of the Convection should be to provide enhanced protection to some categories of data, which, by nature, are broadly accepted as sensitive. Furthermore we believe that processing of non sensitive data that directly or indirectly results to revealing sensitive data should also fall within the scope of the Convention.

(b) We believe that the addition of other categories of data, such as biological or biometric data should be subject to a consensus achieved by the parties. We do not agree that this addition should extend to national identification numbers.

12. Although the intention to provide children with specific protection is quite honorable, in view of the fact that a large percentage of internet users is minors, we cannot see how the application of the new Convention which relates only to automatic processing, can in practice, provide this specific protection. If such a way exists, we are in favour of such a proposal.

13. Yes, but only in case it is decided to adopt an extensive legal instrument, with detailed, rather than general, provisions.

14. Yes, but only in case it is decided to adopt an extensive legal instrument, with detailed, rather than general, provisions.

15. We are however in favour of a general principle that will create an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules.

16. No.

17. Yes.

18. The possibility of introducing provisions for the exercise of the right of opposition and oblivion should be examined.

19. Yes.

20. We move towards a more mild position such as “tracking is permitted subject to condition, ie when this is provided for by law”.

21. Yes.

22. We believe that this issue should rather be addressed in a Recommendation.

23. This notion may be difficult to implement due to administrative law differences among member states.

24. Yes.

25. Most important factors according to which DPA’s independence is guarantied are the following:
(a) Budget and
(b) Personnel
If DPA’s have their own budget and personnel we believe that their independence is ensured.
International cooperation should be ensured in line with article 28.6 of the Directive 95/46/EC.

26. Yes.

27. In our view transborder data flows should be addressed in a new single comprehensive legal instrument which should provide all the necessary details in order to cover all relevant cases (Internet age included) and not in this Convention.

28. The new legal instrument should explore the possibility of integrating international accepted Standards the content of which should be universally accepted and should reconcile effective data protection with the free flow of information.

29. As a starting point No there should be no difference between Private and Public Bodies. Referring to BCR's and the possibility for the Private Bodies to make more use of them it is a time consuming procedure and sometimes may proved inefficient.

30. Regarding the functions and role of the Committee we are of the view that they should be strengthened but this is a primarily budgetary issue and should be better raised upon the competent bodies of the Council of Europe. Such functions could be further developed by means of providing standard setting and monitoring functions. As regards dispute resolution we would like to express a view after we see a more detailed proposal.

CZECH REPUBLIC – THE OFFICE FOR PERSONAL DATA PROTECTION

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

A technologically neutral approach should be retained in order to minimise outdating of the document.
See more in “And you?”

2. Should Convention 108 give a definition of the **right to data protection** and **privacy**?

Introduction of these definitions would be meaningful. However, the difference between data protection and privacy should be explained - see the “And you?” section.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes, it should. The provisions should continue to apply to both sectors and focus on PD processing in the “IIIrd pillar” as well, mainly concerning data processed by the Police.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely **personal or household activity.** Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

The text should not apply to data processed for purely personal or household activities.
The notion of “virtual family” should be defined, namely in respect to the expression of the data subject´s will in context of Web 2.0 and online data processing.

5. The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The definition of “automatic processing” should include explicit mention that collection of data is regarded as processing. No special provision on collection is needed. See “And you?".

The definition of the **controller of the file** should be reviewed: should several criteria be listed YES, should such criteria be cumulative NO, can there be several controllers for one file YES ?
Enforcement of principle of “responsibility” is necessary. The legally transparent responsibility among more than one controller of a file has to be added as a new obligation for the data processing.

6. New definitions may be necessary, such as for the **processor** or the **manufacturer of technical equipment**.

YES

Protection principles

7. New principles could be added to the Convention, such as the **proportionality** principle, which should apply to all operations carried out on the data. Such a principle is also linked to the **data minimisation principle** which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Absolutely, we are in favour of including both principles.

8. Should the question of **consent** be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

YES – in both cases

9. Should the **legitimate processing** be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

YES, it would be useful.

10. Convention 108 does not expressly mention **compatibility in relation to purpose**. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Compatibility in relation to purpose has to be mentioned explicitly.

11. **Special categories of data** which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

YES

12. A specific protection could also be applied to certain categories of data subjects. In particular, **children** may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

The text **should remain age neutral** as it should be in terms of technology.
See "And you?".
However, protection of children and minors should be specially approached in the documents and recommendations devoted to the protection of this age category.

13. Article 7 of the Convention addresses **security** in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of **data security breaches**?

NO – the problem is sufficiently treated by the Directive 2009/136/EC.

14. There are special risks arising from the use of **traffic and localisation data** (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Explicit mention of general PD principles in context of traffic and localisation data should be given. See “And you?”.

15. Should **accountability** mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

YES, and see namely the bullet point 5 above.

16. Should the principle of **privacy by design**, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

The principle of PbD should be introduced.

Rights – Obligations

17. The **right of access** should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the **logic** of the processing?

In the cases at least, where profiling is at stake, the access to the logic should be ensured, i.e. covered by the modernised text. See “And you?”.

18. The **right of opposition** is justified in cases where the data processing is not based on the data subject’s consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

YES

19. Should there be a right to guarantee the confidentiality NO and integrity of information systems YES?

In context of the principle of responsibility – mentioned as an obligation, no right.

20. Should a right ‘not to be tracked’ (RFID tags) be introduced?

YES – in accordance with consumer´s rights; to be connected with privacy by design.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

NO, it has to be in accordance with the Data Retention Directive.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

YES

Sanctions and Remedies
23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

YES
Class actions have to be introduced in the Convention.

Data protection applicable law
24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Yes, it should.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

The definition (aspects) of independence has to be formulated.
The question of "independence" should be discussed during the next T-PD plenary session.
The secretary of T-PD should coordinate summing up and analyzing of the national PDPA suggestions and practices concerning international cooperation between national authorities; T-PD bureau and T-PD secretary should coordinate the cooperation and come up with some suggestions based partly on the experience of PDPA suggestions and practices.

26. Should their role and tasks be specified?

The role of DPAs could be listed, not exhaustively however. Space for national specificity should be provided.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

YES

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

YES

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

1. Sentence YES; 2. sentence NO

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

Coordinating function (see above 25.) and monitoring functions concerning international cooperation.

And You?

Please send us your reactions, thoughts, comments on any (or all!) of the points raised above, or any related issue which you consider important to address in the context of tomorrow's data protection.

First, we have to take into account that not all European countries have ratified the Convention 108, neither implemented its principles, nor are they familiar with them. And second, with regard to the fact that the modernised, amended text of the Convention 108 would call for a new ratification process in the national parliaments, a procedure that can cause delays, raise doubts and - on the side of parties that still did not ratified the Convention – even deepen their hesitation, we are of the view that it would be more suitable to present all the amendments in the form of a **new additional protocol** to the Convention. This solution would allow us to reflect both the technological and legal aspects with more flexibility and without necessity to change the existing text..

The Czech suggestion is based as well on the recognition that the Convention 108 as a precious and, for the personal data protection, basic historical document still values, and its principles have been facilitating the dialog with countries introducing or intending to create legislation protecting personal data of citizens and privacy as a fundamental human right

DATA INDUSTRY PLATFORM

Changes to our last position paper and the questions of the T-PD are marked in yellow colour!

Joint group submission to the T-PD's consultation on the revision of the Convention 108:

Content:

Preface

The signatories of this document call upon the T-PD to take a balanced, differentiating and innovation-friendly approach to the revision of the **Convention ETS No 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Data (of 1981) (known as "Convention 108")**.

As a group of signatories we are convinced that the general concepts and principles of the Convention 108 have stood the test of time well and should therefore be maintained in their entirety without deviation through exception or downgrading in importance. Privacy implications of sector-specific issues or technical innovations however, that have arisen in the intervening period following the development of technology (e.g. the creation of the social media environment) would best be addressed by well-differentiated and/or specific solutions (e.g. self-regulation or codes of practices).

We urge the T-PD to take a balanced view on data protection, and the implication of the related fundamental rights. Effective protection of free speech, press freedom and other media freedoms are binding fundamental rights as well, enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms (please see also the Charter of Fundamental Rights effective for all States that ratified the treaty and are part of the EU). The same applies e.g. to the freedom of arts and science, the right to property or the freedom to conduct a business.

The development and growth of the European Digital Society, innovation, culture, science, democracy, and any economic activity relies fundamentally on reliable and relevant data and the free flow of such data. Informational efficiency is the core fundamental element of any well functioning market and democracy.

Any change to the existing data protection framework will define the data-based competitive landscape for states that ratify the treaty at global scale for years to come. Given, that many of the 38 current states that have ratified the treaty are non-EU countries, the review of the treaty could also be an opportunity for harmonising data protection rules beyond the 27 countries of the EU. The T-PD should be aware of its tremendous responsibility.

As signatories we would like the T-PD to take the following comments on its consultation carefully into account:

A. Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

- The Convention 108 should remain technologically neutral in order to keep enough flexibility towards the development of new technologies and innovation. A more detailed text could lead to a situation where new technologies would not be covered when they arise, and constant changes would be necessary to match the evolution of technologies. The current wording of the Convention 108, based on principles, makes this instrument "future proof" and therefore provides better protection.
- The practical use of innovative technological concepts, such as aggregated data, cloud computing, IP-Addresses, RFID, cookies, and geo data must and can be solved within the existing framework of the Convention's technological neutral approach.

2. Should Convention 108 give a definition of the right to data protection and privacy?

- We believe that Convention 108 could give a definition of Data Protection. However, such a law would effectively try to amend the Convention of Human Rights and Fundamental Freedoms. We think that systematically any clarification of fundamental laws enshrined in Article 8 and Article 10 of this convention should much more adequately be amended to the very same convention, not to the Convention 108.
- The signatories of this position paper are already subject to EU law. Amongst the 27 member states of the EU, the right to data protection became a fundamental right in the Lisbon Treaty of 2007. Article 16 of the Treaty on the Functioning of the European Union lays down a specific and comprehensive legal basis, which is now prominently placed in Title II on "Provisions of general application". The substantive parts of this provision clearly affirm that "Everyone has the right to the protection of personal data concerning him or her" (paragraph 1) and that compliance with data protection rules shall be subject to the control of independent authorities (paragraph 2).

- It is our opinion that any definition recommended by the T-PD should mirror the law of the EU. Any law going beyond the legal standards of the EU would further increase the already existing discrepancy in data protection standards amongst ratifying states. An alignment with the 27 member states of the EU would allow the ratifying states inside and outside the EU to have a harmonized zone of data protection.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

- We strongly believe that this approach should be maintained. Both industry and governments should abide by the same rules.
- Especially when one considers that governments generally collect and process large amounts of sensitive data (income, health, criminal record) and have the means to interconnect these databases. This principle also applies to law enforcement. These days law enforcement often uses governmental data such as tax returns to track suspects. According to the press, law enforcement agencies also make apparently more and more use of data published on social media web sites. The public and private authorities must abide the applicable data protection rules.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

- No comment.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list? The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

- No comment.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

- The current convention provides applicable definitions of parties involved in the processing of data. With the current definitions all parties involved such as processor and controller can be held accountable. We wonder how defining new parties would improve the convention, if the current definitions have proven to be applicable for organization and law enforcement.

B. Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

- We believe that this is not necessary. This convention is subject to the proportionality principle immanent to all of the signatory's actions that temper with its citizens' fundamental rights. The T-PD and eventually the signatory must therefore take a balanced approach on the revision of this treaty.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

- We believe that the principle of transparency is key in the processing of personal data, and consider the obligation to inform as an intertwined part of this principle.
- It is important to set up clear grounds for the processing of personal data. As defined e.g. in the European Directive 95/46/EC, consent is one of the criteria for making data processing legitimate. Data processing is e.g. also allowed when it is necessary for the purposes of the legitimate interests pursued by the controller. This is a legitimate ground for data processing, provided that the consumer is well informed. The signatory has also established specific scenarios on a national level in which data can be processed as by decision of parliament to serve certain needs of society. Making consent obligatory for all data processing would be a disproportional burden for organizations and the signatories' sovereign, its people. It will not benefit the citizen, because it will influence the competitiveness of markets and burden him with decisions better taken by parliament. If new companies can not get in contact with their potential clients, this could severely stifle innovative start ups and small companies.
- As already mentioned, it is our opinion that any definition recommended by the T-PD should mirror the law of the EU. Any law going beyond the legal standards of the EU would further increase the already existing discrepancy in data protection standards amongst ratifying states. An alignment with the 27 member states of the EU would allow the ratifying states inside and outside the EU to have a harmonized zone of data protection.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

- (See answer to question 8)

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

- (See answer to question 8)

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

- We believe that the current categories of data which benefit of increased protection are sufficient.
- Furthermore the existing principles of proportionality make sure that whilst processing data a controller must always take into account the fundamental right to data protection of the data subject. If his processing infringes this right, he can already be held accountable because of a principle based approach of the convention.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

- In this context, parents should be reminded, aided and held accountable for their children's exposure and education towards a responsible use of the internet. In all states that have ratified the Convention 108, it is the custodian's role to supervise and foster children. In parallel, schools and play-schools should cover the risks of internet usage in their curricula.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

- The Data Industry Platform does not see the need to introduce a new rule on data breach notification. The platform is concerned that additional burdens will be imposed on businesses without providing effectively a higher level of protection to data subjects.
- We understand that security of data is of high importance. Data must be protected against unauthorized access and a data subject should be able to trust that his data is secured by a controller. Therefore we are sympathetic to this concept, because it is an incentive to secure personal data. However, we believe that a Breach Notification is an elaboration of the principle of protection against loss. We believe this elaboration should most adequately be addressed in a self-regulation. Self-regulation could aid to develop consistent, practical notice requirements, where needed. These requirements must contain risk-related trigger-mechanisms.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

- The practical use of innovative technological concepts, such as aggregated data, cloud computing, IP-Addresses, RFID, cookies, and geo data must and

can be solved within the existing framework of the Convention's technological neutral approach. Each new technological development must not be covered by specific amendments to the conventions of the Council of Europe, as the revised law would possibly become obsolete as soon as technology or its use changes.
- A technology-neutral approach has the benefits to allow for innovation.
- Self-regulation would be a way to provide solutions to sector specific technical or legal issues that are challenging or need clarification.
- We as industry strongly support self-regulation to tackle these specific areas.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

- Industry trade organizations already have extensive compliance tools to asses their members. Data Protection Authorities have developed several instruments to help organizations comply with privacy law. If regulatory bodies investigate, organizations have a legal requirement to cooperate. Therefore we strictly oppose to make this a legal binding concept. However, should there be an accountability mechanism the T-PD would have to consider the different effects such a mechanism could have on SMEs, large national businesses and global players.
- Data controllers are obliged to comply with data protection laws.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

- We stress the need to maintain a framework with a technological-neutral approach, in order to provide ground for innovation and creative use of technology, therefore achieving a true "Digital Society" in the area of the ratifying states.
- As an industry we already support research and development and best practices concerning privacy enhancing technologies. However, we strictly oppose to make this a legal binding concept. Regulating technologic specifications and standards suppresses and limits the freedom to innovate. This innovation is direly needed to provide consumers with new products and services in an ever more globalized world.
- We believe that the current data protection acquis of the Council of Europe is a very good one and allows industry to innovate.

C. Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

- We do not share the proposal to make here any amendments.

- On the contrary, a new layer of information could be counterproductive as it could confuse the data subjects in the states that ratify the convention.
- There has to be a logical limitation to the data the citizen can obtain. Business secrets, the competitive edge of companies, and their intellectual property must be protected. The signatory must protect the logics of conceptual processing as a crucial business asset of European companies. This includes also internal predictive analysis techniques, which are part of business logics and which may not be revealed to third parties in any circumstances.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

- Concerns regarding social networks and the closely related discussion about a "right to be forgotten" should not be tackled in the Convention 108. These issues should not blur the general and time proven principles. In the sphere of social media the data controller (i.e. the citizen participating in his Web 2.0 activities) has to be accountable for his doings.
- For example, a "right to be forgotten" applying to the media sector would be detrimental for maintaining extensive news archives and press libraries, which are an indispensable resource for high-quality news content, as well as providing important historical records.
- Another example where a "right to be forgotten" is highly questionable, is when a citizens notifies a company that he/she withdraws his/her consent from receiving advertising. If a company has to delete the complete data of the citizen, it will simultaneously not be able to comply with the content of the aforementioned notification.
- Any "clarification" of a so-called "right to be forgotten" should therefore carefully take into account unforeseen negative impact on legitimate business interests and legal obligations from such disperse areas as tax, accounting, warrantee and product recall documentation, etc.
- Concerning the right to "erase data related to a data subject's protective sphere", necessary journalistic exceptions must be allowed for. Reporting should be free from interference of data subjects. Historical archives should be spared from possible corrections not representing the facts. A democratic society can in no case afford the risk of falsification and adaptation of public remembrance. Concerning the "right to rectify" we do not think that there is any legislative gap (e.g. for linear audiovisual services there is a specific rule in the Audiovisual Media Services Directive of the EU).
- However, should any such concept become part of the Convention 108, we strongly advocate to limit any such legal instrument in this area to specific services which are based on data the citizen provide themselves and that make this data available to third parties as an essential part or nature of that service. Such a limitation would leave basic B2C and B2B customer data and data that is of interest to the journal and press sector etc. out of the scope of right to be forgotten.
- We would also highlight that any provisions in this area would have to consider also the technical feasibilities and the proportionality of any such laws.

19. Should there be a right to guarantee the confidentiality and integrity of information

systems?

- No comment.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

- No. The current provisions of the convention and its national implementation in the states that ratified the convention are sufficient. Special self-regulatory regimes can be devised in the future in areas where needed. If the convention limits the technological development pre-emptively in this field, many technological advantages are likely to never develop. The convention must stay technology neutral to stand the test of time and to allow for innovation.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

- Does the offline world truly know a default mechanism or right to remain anonymous in any of life's normal circumstances? We do not see any reason why there should be a distinction between the online and the offline world (e.g. a public library's administrative staff knows the users of the library and can observe their reading preferences as well. To satisfy the needs and wishes of its users it will procure more media of any area of interest in which demand is higher. The users of the library thus strongly influence the media offered.)

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

- No comment.

D. Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

- We do not see the need for the introduction of a collective redress system. Within the signatory we already have a high level of consumer protection and a solid judicial system. Introducing this instrument would possibly weaken the legal position of individual citizens of the signatory in the long view. However, the European principles related to the "Rechtstaat" aim at granting the individual rights and obligations. Citizens, and not any collective or agency, should remain the focal point of our society's constant struggle to improve the signatories legal system.

E. Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

- In general, provisions on applicable law must foster one of the core principles of the data protection framework of the signatory, the principle of free movement of personal data. The current Convention 108 ensures a high, adequate level of protection of personal data, irrespective of where in the reach of the signatory data are physically stored or where the data controller (or data processor) is established. We are convinced that the current rules on applicable law are effective.
- However, we strongly support any practical simplification for companies that engage in European or international cross-border activities. This applies especially to companies that form a part of group of consolidated companies or that operate within an established international network of companies with a common value stream or operating in a common supply chain (e.g. outsourcing companies).

F. Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

- The current provisions of the convention and its national implementation in the member states that ratified the convention are sufficient.
- We think that e.g. the jurisdiction in the European Union sets a clear indication on what is necessary to have independent authorities.
- The signatories of this document would like to add that truly independent authorities should be supervised by a Board that is a stratified sample of the countries main political interest groups.

26. Should their role and tasks be specified?

  - No comment.

G. Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

- No comment.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

- As already mentioned above, we strongly support any practical simplification for companies that engage in European or international cross-border activities. This applies especially to companies that form a part of group of consolidated companies or that operate within an established international network of

companies with a common value stream or operating in a common supply chain (e.g. outsourcing companies).

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

- The related fundamental rights were established to protect the individual and his or her liberties from governmental institutions. We do see the necessity to protect consumers adequately in the context of data protection and data privacy in the private sector. Especially the developments of the Web 2.0 have contributed heavily to the current political discussions about data protection in Europe. However, we think that data protection is first of all a protection of the private individual from the state and an access right against the state. These aspects of data protection are an essential element of European democracies in the 21st century. This protective and political dimension should never be diminished by any shift of attention.
- Corporate rules should only be binding in the context of self-regulatory codes. This is no area where the signatory should interfere.

F. Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

- It is our opinion that there are no problems related to this in the current convention. Such activities are likely to double the work of institutions at other levels that are already undertaking them. It would not make sense to add another layer.
- Standard-setting, dispute resolution, and monitoring functions are areas in which self-regulation is the most adequate solution.

FK CONSULTING

The Danish Personal Data Protection Act (based on the EU data protection directive of 1995) defines the data controllers "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of information. " (§ 3, 4). Likewise, the law stipulates that if a natural or legal person, public authority, agency or any other body is dealing with information on behalf of the controller, he is called "data processor"(see § 3, No. 5).

In my view, any organization (public or private) of a certain size (e.g. 50 employees) should be obliged to appoint a so-called data protection responsible person, because responsibility is hereby made clearer and more understandable when it becomes personified. Both the controller as well as the processor should be required to undergo certified training on data protection and privacy. For comparison, several European countries have an education as Data Protection Officer, who is a protected title. The training could very well be part of a broader credit cycle with eg information security, human rights and others including at the bachelor / master level.I recommend that The Council of Europe takes initiative to launch a Pan-European education program in data protection and privacy starting with a feasibility study of the current European landscape of data protection and privacy courses and education programs.

EBF

D0447A-2011
09.03.2011

Set up in 1960, the European Banking Federation is the voice of the European banking sector (European Union & European Free Trade Association countries). The EBF represents the interests of some 5000 European banks: large and small, wholesale and retail, local and cross-border financial institutions.
The EBF is committed to supporting EU policies to promote the single market in financial services in general and in banking activities in particular. It advocates free and fair competition in the EU and world markets and supports the banks' efforts to increase their efficiency and competitiveness.

EBF POSITION ON THE CONSULTATION ON THE MODERNISATION OF CONVENTION 108 OF THE COUNCIL OF EUROPE (AUTOMATIC PROCESSING OF PERSONAL DATA)

The European Banking Federation (EBF) would like to thank the Council of Europe for the opportunity to comment the consultation on the modernisation of Convention 108 with regard to automatic processing of personal data.

The Convention deals with complex issues that have relevance to the European financial services sector. We are therefore grateful to be able to comment them[1] and lead to our final goal on the issue of data protection: legal certainty for the processing of European banks' customers' data.

The EBF would favour a framework of the Council of Europe that would address the below highlighted answers. This would be for the benefit of European banks and their customers whose data continue to be processed as securely as possible.

[1] The EBF answered only questions of the consultation related to issues of specific relevance for the European financial sector and where a consensus could be found within EBF membership.

European Banking Federation (a.i.s.b.l.)
10 Rue Montoyer B-1000 Brussels
T: 32 (0)2 508 37 11
http://www.ebf-fbe.eu

EBF Position on the Consultation of the Council of Europe on the Modernisation of Convention 108- Automatic Processing of Personal Data

Object and Scope of the Convention - Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

The EBF believes that the Convention 108 should stay technologically neutral in order to remain an international legally binding instrument with the potential to be applied worldwide.

However, certain adaptation may be necessary for the use of personal data in the context of internet, in particular with the deployment of web 2.0.

2. Should Convention 108 give a definition of the right to data protection and privacy?

Yes, Convention 108 should give a definition of the right to data protection and privacy. This should be particularly the case as Convention 108 will serve as a basis to countries outside the European Economic Area which have no specific definitions in their own legislation, and would have no knowledge of the evolution of "privacy" and "data protection" in European institutions' case-law and doctrine in line with existing European definitions.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes, EBF members believe that the comprehensive approach of Convention 108 should be retained.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list? The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

EBF members would be in favour of changing the definition of "automatic processing" to "processing" with a definition being in line with that of Article 2b [2] of Directive 95/46/EC rather than "collection" being subject to a special provision.

Regarding the definition of the controller of the file, it should be added that there can be several controllers for one file (controller of the file means the natural or legal person, public authority, agency or any other body who alone or jointly with others (...)). However, we do not think that the definition of controller of the file in Convention 108 needs to be more explicit on this point. Consideration should be given to the changes in the way data is collected, used and processed in the age of the internet and cloud computing, to ensure that the terminology is not confined by concepts of "file" or other technology specific mechanisms which may compromise the neutrality and hence broad applicability of Convention 108.

[2] 'Processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

At least one definition should be added: "processor" (natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller).

A nuance may be necessary for service providers processing data on behalf of the controller but enjoying a clear autonomy to realise the service so that they bear a double cap of "controller of file" and "processor". In that case, the notion of "person entrusted" with the processing could be introduced: where the sub-contractor is acting strictly on behalf and upon instructions of the data controller and is not responsible as a data controller, the person entrusted with the processing may be considered as bearing part of the liability, jointly or wholly.

It is a good approach too to add a definition of "manufacturer of technical equipment".

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Article 5 of the Convention already states that data shall be adequate, relevant and not excessive in relation to the purposes for which they are stored, and that the data shall be stored for specified and legitimate purposes. Thus, the principle of data minimisation / proportionality is already taken into account, even if there is no explicit manifestation of it.

It is important not to set rules that are overly prescriptive in this area since they may conflict with the operating requirements or legal/regulatory obligations European banks are subject to and which facilitate the operational efficiency of their business. European banks are best placed to determine what personal data they need to keep and for how long in view of their legal and regulatory obligations.

Minimisation should be referred to only if linked with proportionality, but not as a separate principle.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

The question of consent should indeed be considered as a legitimate ground for the processing. Consent is however a very fragile ground since it can be withdrawn at any time (and then there is no more legal ground to the processing).

However, the question of consent should not be a necessary prerequisite to a fair and lawful processing.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its Article 7? Should there be a list of legitimate grounds for data processing?

Yes, a list of legitimate grounds for data processing could be useful.

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection

Even if Convention 108 does not expressly mention compatibility in relation to purpose, this principle is showing just beneath Article 5 of the Convention.
Moreover, it should be specified that data initially collected for one purpose can be reused for another purpose only if this second purpose is closely linked to the initial purpose (e.g. debt recovery for data initially collected for purchase of a service or a good).

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

EBF members do not think that Convention 108 should introduce a specific right for individuals to be informed of all data security breaches. We feel this would be an overly prescriptive measure and would add no additional protection to individuals or prevent breaches from occurring.

Financial institutions fully understand there are circumstances that require notification to financial and/or data protection regulators and affected individuals in the event of a breach. Many financial services regulators already require financial organisations to report specific types of breaches and it is important not to be operating in a dual regime, which could either provide for duplicative or conflicting obligations.

It is also important to look at the lessons learned in countries where an overly prescriptive breach notification regime has failed to meet its objectives, and has instead created confusion and unnecessary alarm to individuals, or where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

No, general rules are sufficient to regulate the use of traffic and localisation data.

Rights – Obligations

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

The right of opposition should indeed be explicitly mentioned in the Convention.

The right to oblivion is one of the most difficult topics under current consideration and perhaps the one most affected by advances in technology. It is a key area where social norms are not yet established and where practical application will be extremely difficult and not always appropriate.

The right to be forgotten cannot be absolute in all circumstances. There are many legitimate, including legal, reasons why a financial organisation should justifiably be able to keep records of its interaction with the individuals it interacts with, even if they might prefer those records to be deleted, e.g. continuity of business, management information and records, employee references and historical records.

Sanctions and remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

The debate on class action and the possibility for a legal entity to bring an action before a court is not a debate specific to data protection. This debate should thus be addressed separately in a more general context.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Yes. It is indeed convenient to wonder about the interest of a possible harmonization of private international law in this context, and to determine which role could possibly have the Council of Europe in this respect.

Data protection authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

Data protection authorities should have more resources.

International cooperation between national authorities could be facilitated with the elaboration of international mechanisms intended to facilitate the cross-border cooperation for the application of data protection laws.

26. Should their role and tasks be specified?

Yes.

Trans-border data flows

28. Do we need to reconsider the notion of "trans-border data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

It is indeed necessary to clarify the concept of trans-border data flow, particularly in the context of internet. This is of utmost importance for banking groups with cross-border activities striving for a coherent group policy and processing of data.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

No, minimum requirements should be the same for private and public sector. Indeed, more use should be made of binding corporate rules, in particular within international companies. In order to help companies to implement such binding corporate rules, mutual recognition should be encouraged.

EBU

European Broadcasting Union Union Européenne de Radio-Télévision

Legal Department ***Département juridique***

EBU·UER

03.03.2011
ACB

EBU comments concerning the Council of Europe's questionnaire regarding the modernisation of Convention 108.

The EBU welcomes the consultation and is grateful for the opportunity to contribute to this important debate.

By way of introduction and given that the Council of Europe and the European Union share the same concerns, challenges and objectives regarding the review of their respective texts (i.e. Convention 108 and Directive 95/46/EC), we invite the Council of Europe to read our contribution (appended hereto) on the same topic, which was sent to the European Commission on 14 January 2011 in the context of the review of Directive 95/46/EC.

The protection of privacy and personal data protection are an important legal and political concern in today's information society, and particularly on the Internet and with the development of new online services and applications (i.e. social networking, user profiling, online behavioural advertising and cloud computing) which give rise to new challenges for the protection of personal data.

At this stage, referring to the Council of Europe's questionnaire the EBU would like to focus on one particular question: *"22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?"*

It is indeed correct that Convention 108 does not have for the time being an explicit journalistic derogation from certain data protection rules such as Article 9 in the EU Directive 95/46/EC.

Article 9 (2) (b) - Exceptions and restrictions- of Convention 108 states: "*Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of - b) protecting the data subject or the rights and freedoms of others."*

Point 58 of the explanatory report states that this provision may concern major interests of third parties, such as freedom of the press.

However, the provision is not sufficient and should be explicitly reinforced to give a clear exemption to journalistic activities, and particularly in the audiovisual field, from the application of certain data protection rules.

Accordingly, Article 9 paragraph 2 of Convention 108 should be amended as follows:

Proposed new Article 9 (2) - "*(c) protecting the processing of personal data carried out solely for journalistic purposes* ".

EBU·UER
Case postale 45 L'Ancienne-Route 17A
CH-1218 Grand-Saconnex
Switzerland / Suisse

Tel +41 (0) 22 717 2505
Fax +41 (0) 22 717 2470
Internet //www.ebu.ch

It is essential for the fundamental human right of freedom of expression and the proper working of the media, and not least in the new technological environment, to ensure that the provisions of the Convention cannot be used to obstruct the exercise of journalistic activities and the fulfilment of the media's role in democratic societies. The necessity and importance of *a new Article 9 (2) (c)* of the Convention will increase as the technology delivering the media becomes increasingly complex and ubiquitous.

For the EBU, it is vital, in the interests of media freedom, investigative journalism and the confidentiality of journalistic sources, for this explicit exemption for media and journalism to be adopted in a revised Convention.

The balance between the protection of personal data and other fundamental rights, such as freedom of expression and media freedom, needs to be kept at the heart of any review of data protection rules.

_____

1 Annexe

14.1.2011
DAJ/ACB/ave
English only

ANNEXE

EBU comments concerning the consultation on the Commission's Communication "A comprehensive approach on personal data protection in the European Union"

1. The protection of users' privacy requires particular attention in the new media environment

The protection of privacy and personal data protection is an important legal and political concern in today's information society, and particularly on the Internet and with the development of new online services and applications (i.e. social networking, user profiling, online behavioural advertising and cloud computing) which give rise to new challenges for the protection of personal data.

As regards the traditional (one-way) free-to-air broadcasting environment, radio and television reception, listening and viewing are anonymous, and users' personal data are not collected. Viewers and listeners would probably welcome an unchanged level of data protection when television and radio services move to new technical platforms or become hybrid, i.e. combining linear programmes with non-linear online content. They are, however, aware that in the age of digital media and new delivery platforms the collection of personal data is a common feature and that a higher level of collection and use of personal data is an irreversible process. That is why data protection rules are becoming ever more important and it is even more important for viewers and listeners to be fully informed in advance of the data collected, and the purpose and identity of data necessary to access certain services. Transparency becomes one of the key factors in data protection.

Today, the reception of radio and television content and services is changing. The Internet, as well as closed proprietary platforms, is now an essential means of delivering media services to consumers and interacting with audiences in unprecedented ways. However, free-to-air radio and television services should be as accessible as possible without any need for personal data from users. If, however, the access to certain services requires personal data, the user should be informed exactly what kind of data are being collected by whom and for what services and purposes.

In addition, broadcasters should be able to access and exploit data on users' viewing/usage (behaviour and habits) in connection with their audiovisual media services, necessary for legitimate usage, i.e. audience measurement, parental control and for adapting offers to users' needs and preferences.

In an increasingly complex technological environment with, for instance, the development of Internet-connected or hybrid TV, the EBU therefore fully supports the

EBU·UER
L'Ancienne-Route 17A
Case postale 45
CH-1218 Grand-Saconnex GE
Switzerland / Suisse

Tel +41 (0)22 717 25 05
Fax +41 (0)22 717 24 70
e-mail daj@ebu.ch
Internet www.ebu.ch

Commission's approach to increasing transparency, as a key element in data protection. It is essential for the consumer to know exactly what kind of data are collected by whom and for what purposes. However, attempts to extend the rules applicable to personal data to non-identifiable anonymised data not identifying the individual could undermine innovation and the commercial and public service viability of the Internet.

Moreover, even though the 1995 EU Data Protection Directive has, overall, worked effectively, the EBU is of the opinion that certain key concepts should be clarified (i.e. personal data, consent, sensitive data, and the right to be forgotten) and that the revision of the Directive should also look at areas of inconsistent application in the different Member States.

It is also the EBU's view that the underlying principles of the concept of "privacy by design" are a highly pertinent solution for the protection of personal data which should be investigated further and integrated or embedded at the very earliest stage of deployment of, for instance, social networks and hybrid broadcasting systems.

Ultimately, there is a need to ensure that data protection is effective to sustain public trust in new media, but it also needs to be regulated in a way which does not hamper the competitiveness of European industry online, or its ability to provide new and innovative products and services to the European media consumer.

2. The derogation for journalistic purposes in Article 9 of Directive 95/46/EC needs to be maintained and reinforced

At this stage, the EBU would stress, as a general point, that any forthcoming legislative proposal should be balanced and take into account all stakeholders' interests. This relates, in particular, to the relationship between the protection of personal data and other fundamental rights, such as freedom of expression and media freedom.

With specific reference to journalism and freedom of expression, Article 9 of the Directive provides that "Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely *for journalistic purposes* or the purpose of artistic or literary expression *only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression*" (see also Recitals 17 and 37).

This has been supported and further developed by the European Court of Justice in its judgment of 16 December 2008, C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy. The Court stated that the purpose of Article 9 is to reconcile two fundamental rights: the protection of privacy and freedom of expression. The obligation to do so lies within the competence of the Member States.

Furthermore, the Court took the view that "in order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly", although this

must not have the effect of encroaching unnecessarily on the protection of the fundamental right of privacy.[1]

To reconcile those two fundamentals rights, Member States are required to provide for a derogation from certain data protection rules where personal data are processed solely for *journalistic purposes* and only if it *is necessary to reconcile the right to privacy with the rules governing freedom of expression.*

A specific example of this balance can be seen in the drafting and implementation of the "right to be forgotten". The right of the individual to control his private information needs to be separated from the capacity to alter or disappear from the public record. The media's role in providing that public record needs to be protected for the benefit of society as a whole. It should also be noted that in an increasingly complex online world it is not even a simple matter to define journalism, or where the boundaries of journalistic organisations lie. The protection of Article 9 is vital to a democratic society, but it needs defining in a manner that will be understood in a complex digital world.

It is essential for the fundamental human right of freedom of expression and the proper working of the media, and not least in the new technological environment, to ensure that the provisions of the Directive cannot be used to obstruct the exercise of journalistic activities and the fulfilment of the media's role in democratic societies. The necessity and importance of Article 9 of the Directive will increase as the technology delivering the media becomes increasingly complex and ubiquitous.

For the EBU, it is vital, in the interests of media freedom, investigative journalism and the confidentiality of journalistic sources, that this explicit exemption for media and journalism should at least be preserved or maintained and, where appropriate, reinforced, in a new data protection Directive. The objective is also to ensure that Member States correctly provide for a derogation upholding freedom of expression and also adopt a broad interpretation of "journalistic purposes" in accordance with the ECJ judgment of 16 December 2008.

The balance between the protection of personal data and other fundamental rights, such as freedom of expression and media freedom, needs to be kept at the heart of any review of data protection.

---

[1] Accordingly, the Court defined the notion of "journalistic activities" referred to in Article 9 of Directive 95/46/EC as encompassing all activities whose object is the disclosure to the public of information, opinions or ideas, irrespective of who is carrying on such activities (not necessarily a media undertaking), of the medium which is used to transmit the processed data (a traditional medium such as paper or radio waves or an electronic medium such as the Internet) and of the nature (profit-making or not) of those activities.

EFAMRO - ESOMAR

Council of Europe consultation on the modernisation of Convention 108

9 March 2011

This paper is submitted on behalf of EFAMRO, the European Federation of Associations of Market Research Organisations and ESOMAR, the World Association of Research Professionals.

Founded in 1992, EFAMRO represents the interests of market, social and opinion research in Europe. Its members are national trade associations for research businesses.

Founded in 1948, ESOMAR gathers together nearly 5000 individual members worldwide on both the provider and client side as well as in public bodies and academic institutions.

Introduction

EFAMRO and ESOMAR welcome the opportunity to respond to the Council of Europe's consultation on the modernisation of Convention 108. We have consulted with key stakeholders in the market, social and opinion research sector not only in Europe but across major global markets in the preparation of this response. We confirm that the contents of this paper are not confidential and can be attributed to EFAMRO and ESOMAR.

We note that the 30 consultation questions cover many topics with potential impact for our sector and due to the relatively tight response deadline we have concentrated on the topics which appear, at this stage, to be of the most particular concern to the research sector. It should be noted that we are interested in the whole of the data protection consultation and would wish to be involved in any of the broader discussions that the expert committee set up under Convention 108 (the T-PD) will hold, not just the topics which are covered in this response.

Market, social and opinion research

Research in itself does not seek to change or influence opinions or behaviour. Unlike direct marketing, advertising or other commercial communications, it does not seek to promote the aims or ideals of those who conduct or commission it. While research is used by marketers to test their products or messages, it is not a commercial communication.

Market, social and opinion research plays a key role in helping businesses and other constituencies better understand consumers, customers and citizens in developing goods and services and is essential for economic efficiency, innovation and progress. Social and opinion research is widely used by public bodies to understand citizens' preferences and measure key performance indicators, for example the Eurobarometer surveys carried out by the European Commission, and government studies used for improving educational, healthcare and police services.

Market, social and opinion researchers adhere to self-regulatory codes of conduct covering a range of data protection and privacy issues. Since the 1940s, market, social and opinion research has been robustly self-regulated by a family of codes of conduct and practice, supported by strong compliance and disciplinary frameworks. Amongst these, the ICC/ESOMAR International Code on Market and Social Research (last updated 2007) is used in 17 EU Member States and 58 associations in 47 countries internationally.

The fundamental principles of research, shared by the ICC/ESOMAR International Code and other codes used by national associations are that:

- Research must be conducted with the voluntary cooperation of respondents, based on the principle of informed consent.
- Respondents must not be harmed or disadvantaged as a result of participating in a research project.
- Personal data collected for research purposes must not be used for other purposes.

These principles mirror those of Convention 108. We also note that the Council of Europe has developed similar conditions which apply to research in its Recommendation No. R(97) 18 (hereafter "R(97) 18") concerning the protection of personal data collected and processed for statistical purposes. ESOMAR raised this issue with the T-PD in 2010 during the development of the *Recommendation On The Protection Of Individuals With Regard To Automatic Processing Of Personal Data In The Context Of Profiling*. Data collected and processed for statistics are already subject to more detailed provisions in R(97) 18. The Recommendation covers a number of issues raised in the current consultation's questionnaire, including consent, sensitive data, rendering data anonymous, rights of access, communication of data for non-statistical purposes, conservation of data for research quality checks, rules for transborder data flows and security of personal data. In particular, we note the following points are recognised by R(97) 18:

- Research assists both public and private bodies in decision-making and promotes the advancement of knowledge.
- Research is valuable whether carried out by public or private/commercial bodies. Research by commercial organisations should not be treated differently than research by public bodies (the latter which we would understand to include universities etc.)

- Research results designed to "characterise a collective phenomenon" mean that the emphasis is not placed on the significance of the individual's personal data. The Convention should recognise the fundamental distinction between the individual use of personal data and their collective use.

- Paragraph 14. b. of the Explanatory Memorandum of R (97) 18 notes that "every effort is made to ensure the least possible disruption for the individual through the actual gathering of the information." Research codes of conduct require that data collection is relevant and not excessive and, further, that individuals are protected from harm or adverse consequences of participating in a research project.

- Data collected for research purposes must only be used for research and not used or communicated for other purposes. This is also a key requirement in market, social and opinion research codes of conduct and guidelines.

- Processing of data for research is systematically followed by a quality control back-checking phase, therefore automatic processing of information which identifies individuals can legitimately also be used for the related purpose of quality control.

Our numbered responses correspond to the question numbers in the consultation document.

1) Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

While EFAMRO and ESOMAR would support provisions that relate to specific organisational measures, we do not believe that the revised Convention should contain specific technological provisions, as this would impair its technology neutral status.

A technologically neutral approach remains relevant. Similar to Directive 95/46/EC, the Convention sets out principles that are independent of media or techniques. This provides flexibility in allowing for the interpretation of the principles appropriate for each platform or technique. It also provides a role for self-regulation. In the context of market, social and opinion research, codes of conduct and guidelines are regularly reviewed and adapted quickly to reflect social or technological developments. These support the necessary and ongoing re-interpretation and application of the principles in a rapidly changing technological environment.

5) The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

EFAMRO and ESOMAR recommend that collection should not be subject to a special provision, but rather included in the definition of processing in the Convention. This would align the Convention with Directive 95/46/EC which includes collection as part of "processing" in Article 2(b):

> *'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;*

Convention 108 also differs from Directive 95/46/EC as it defines the controller as the person who determines the purpose of the automated data file, rather than the EU's definition of the controller as the person who determines both the means and the purpose of the processing of personal data.

The preferred solution would be to harmonise these definitions. In our submissions to the European Commission, we have advocated for the introduction of a clarified definition of data controller which would place responsibilities on those who decide how data are processed as opposed to those who control a particular computer or filing system.

This would restate the responsibility of a single data controller to assess the need to process personal data and the security of such systems before electing to process personal data in them and would provide a single point of responsibility and accountability to citizens. Since the operator of a particular computer or filing system would be contractually bound or otherwise obliged to abide by their representations about system integrity to those who use their systems for processing data, there is no disruption to the continuity of data protection.

A clarified definition of data controller would also restate the responsibility of data controllers to assess the security of such systems before electing to process personal data in them. Clarification of this definition would furthermore serve to increase harmonisation across the Member States.

In the market, social and opinion research context, data may be processed by a telephone centre, a website and by research analysts as part of the same project. Each section or part may work within separate entities and hold data in separate systems. Process standards (such as ISO 20252[1] and similar national standards) and ethical standards (codes of conduct and practice) ensure that each aspect is managed consistently and that respondents are protected. A single data controller assists the protection of individuals as there is a single point of responsibility and accountability. The phenomenon of multiple controllers decentralises this function and increases the risk of errors occurring.

[1] ISO 20252:2006 establishes the terms and definitions as well as the service requirements for organizations and professionals conducting market, opinion and social research.

6) New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Further to our response to question 5 above, EFAMRO and ESOMAR do not believe that new definitions are necessary for processors or manufacturers of equipment. The primary responsibility for the protection of personal data should rest with the data controller. Data controllers should be free to make properly informed decisions about the processors or technology they use.

7) New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

EFAMRO and ESOMAR believe that the emphasis in the Convention should be on responsible data collection and data minimisation, retaining data only where it is necessary for the purpose for which it is collected.

In research, the International Standard for market, social and opinion research, ISO 20252, the development of which was strongly supported by EFAMRO and ESOMAR, sets down retention periods for data collected or generated in the course of research projects and this is also reflected in the sector's self-regulatory codes. The purpose of these retention periods is to allow for necessary processes such as quality control and verification of results. These are essential activities to ensure research is robust and representative, and undertaken whilst balancing this with not keeping data longer than is necessary once the process has been fulfilled. The Convention should support and encourage the development of such policies and practices by data controllers.

8) Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

EFAMRO and ESOMAR believe the requirement for unambiguous consent is sufficient as currently exists in the EU Directive 95/46/EC but should be clarified for consistency of application. Unambiguous consent requires data subjects to clearly be informed about the data that is being collected about them, who will have access to it and what it will be used for. We consider this level of consent to be sufficient to ensure that data is adequately protected.

In many cases, unambiguous consent is obvious – in research a respondent to a research project provides the answers to the questions they are asked, having been informed of the identity of the researcher, the purpose of the interview, and of their right to withdraw at any time. There is no specific question to obtain permission for the processing of data, but the consent of the data subject is unambiguous nonetheless from the circumstances of the data collection.

Only in cases where data processing is not obvious or where further processing is intended at a later date would additional information need to be provided and consent obtained by the asking of a specific question. The interpretation of explicit consent has varied from jurisdiction to jurisdiction and should not be interpreted as written consent as this would introduce a disproportionate administrative burden and hamper the collection of responses for market, social and opinion research. For example, in Europe, telephone research is an essential tool in discovering and understanding the views of hard-to-reach groups, such as geographically isolated communities, individuals with disabilities, or the elderly. A requirement for written consent, not possible in telephone communications, would deprive these respondents of their right to be heard, and deprive research users' access to important research findings.

An over-emphasis on consent has led to a distortion of the concept as it is used in a one-size-fits-all approach. Insisting on explicit consent for every data collection event and not just sensitive data events will embed an "always click yes" mentality in data subjects. By treating all consent in a formulaic way the value of consent overall is diminished and may in fact mean that data subjects are less protected. Further, requiring explicit consent in all cases would place disproportionate burden on both the data subject and the data controller. Such a burden is restrictive and not enabling – it impedes the flow of data without a commensurate increase in the protection of the rights of the data subject. For research, requiring explicit consent for every data collection event would reduce response rates and levels of unbiased results and thus the possibility to achieve accurate sampling on which quantitative research is based. The fundamental principles of research, shared by the ICC/ESOMAR International Code and other codes used by national associations are that research must be conducted with the voluntary cooperation of respondents, based on the principle of informed consent.

If the question of consent is considered for inclusion in Convention 108, then this should be informed by current discussions on the revisions of Directive 95/46/EC. Consent is currently considered at EU level as the first of six conditions set out in Directive 95/46/EC for fair and lawful processing in Article 7. Current EU rules have generated a lack of clarity about the other five grounds for fair and lawful processing currently in Article 7.

9) Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

EFAMRO and ESOMAR would welcome the introduction of a ground for legitimate processing in Convention 108. We would not support an exhaustive list of legitimate grounds for data processing.

If the Convention decides to include a provision on allowing processing where it is necessary for the purposes of the legitimate interests pursued by the controller as the EU currently does in article 7, a harmonised approach would be necessary. We would note that processing data for market, social and opinion research does not directly affect the rights or freedoms of the data subject (indeed by giving citizens a voice, research strengthens the democratic rights and freedoms of European data subjects). We believe that this condition can be appropriately

applied, for example, to the use of publicly available information to form robust and reliable sample frames for research.

10) Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

In the revision of the Convention, market, social and opinion research should not be considered as incompatible with the initial purpose of the data collection. This is already recognised in the R(97) 18 subsequent to the Convention and in Directive 95/46/EC Article 6, paragraph 1.b)

> *Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered incompatible provided that Member States provide appropriate safeguards.*

EFAMRO and ESOMAR recommend that a similar provision is introduced in a revised Convention.

Market, social and opinion research supports decision-making and this research in itself does not seek to change or influence opinions or behaviour. The fundamental principles of research, shared by the ICC/ESOMAR International Code and other codes used by national associations are that personal data collected for market, opinion and social research must not be used for other purposes. This in turn limits all processing of the data, and the extent to which it may be further processed and accessed.

Once collected for research, data relating to identifiable individuals may be processed further as part of quality control and verification. This protects the robustness of research results by ensuring for example that individuals or groups of individuals cannot bias research projects by submitting multiple or fraudulent responses. As more research moves to online environments, this kind of processing will become more necessary to guarantee the quality and robustness of European research and statistical data, vital to the development of the European economy and as such should be recognised as a legitimate purpose. We would note that R(97) 18 recognises that "identification data used as ancillary data" is an integral part of the production of statistical results.

11) Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

We do not see the need to add other categories of data to the list of sensitive data and recommend that these should be harmonised with the EU Directive. However, we consider that additional clarity regarding the scope of what constitutes sensitive data would make compliance simpler.

As an additional point, we are aware that in some countries, data protection supervisory authorities are required to give their prior consent before sensitive personal data can be obtained from data subjects. The differences in the way that additional safeguards are applied by domestic authorities to special categories of data hampers the conduct of market, social and opinion research and does not add to the protection of individuals.

EFAMRO and ESOMAR believe that obtaining the free and explicit consent of the data subject for the processing of this information offers sufficient protection and control to the data subject. Further requirements of third-party authorisation of the data collection would place an unwarranted burden on research and its ability to produce robust and valid data for the benefit of European businesses, governments and citizens.

12) A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

The Convention does not explicitly contain provisions for the protection of children; nevertheless many sectors including market, social and opinion research have actively introduced additional rules to ensure the adequate protection of children and young people who are not yet adult. This includes all the relevant self-regulatory research codes in Europe. The protection of children and young people should not be over-simplified to a mandatory requirement for parental or guardian consent for contact with all individuals under 18 nor should children's data be classified as sensitive data in the revised legislation to reflect this consideration.

Persons under 18 may leave school, or attend university and are autonomous persons. The UN Convention on the Rights of the Child also guarantees right to express views to participate in society:

Article 12: States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.

Article 13: The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.

If additional measures were to be introduced, the need to address concerns for the protection of children and young people must be balanced with their rights of expression. Children have the ability to take decisions that are appropriate to their competence, environment and corresponding to their age, whilst noting for example it would not be appropriate to expect a child to take transactional decisions usually taken by the head of the household.

We recommend that if additional restrictions were to be introduced that these mirror the self-regulatory rules already in place, the majority of which require consent or supervision of a responsible adult such as a parent or guardian with under 14s. It is our view that if we are to properly prepare children and young people for the transition from childhood to adulthood that the transition should start at 14 not 18. For those over the age of 14, it is generally accepted that they can provide personal information for research as a young person can make an informed decision and take into account the consequences of providing that information which does not involve a personal obligation.

This will depend on the sensitivity of the survey topic. Existing self-regulatory rules and guidelines require researchers to seek parental consent on more sensitive topics providing this does not conflict with the interests or rights of the young person.

16) Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

EFAMRO and ESOMAR support enabling citizens to decide how and when their personal data should be collected and processed. This is reflected both in the fundamental principles of research and in the practical application of research codes of conduct and practice. Privacy and data protection should be a key design consideration in the development and application of new information technologies. Examples include:

- Default settings in social networking sites that protect privacy while allowing citizens to choose lower levels of privacy if they wish;

- Transparent, understandable and comprehensive privacy policies that provide citizens with information that they need to know before their personal data are collected and processed.

EFAMRO and ESOMAR support the principle of privacy by design forming part of the technical and organizational measures required to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. This is particularly important where the processing involves the transmission of personal data over a network.

The application of this principle should however allow for relevant and necessary use of information in relation to the risks of the technology used. The application of the principle should also be technology neutral. New technologies should not be subject to either a higher or lower standard of scrutiny than technologies in current use. This would inhibit the development of new technologies necessary for the development of the EU economy and of innovation in the research sector.

There is a need for greater understanding and appreciation of current privacy and data protection practice in the design and application of new technologies before specific new requirements are put in place. This is necessary to

avoid discouraging technological development; the Convention should strive to encourage innovation while protecting the rights of citizens.

Code holders, trade bodies and other organisations can encourage this protection by ensuring that privacy and data protection features are designed into new developments and form part of the compliance framework for that sector. In research, EFAMRO and ESOMAR already require this of their members.

18) The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

As we have noted above, research must be conducted with the voluntary cooperation of respondents, based on the principle of informed consent. This provides individuals with a natural right of opposition to data processing for research purposes. Further, data relating to identifiable individuals is generally held on a time-limited basis by research companies, so respondents are soon "forgotten" by research organisations. A possible exception to this is access panels, which hold data on individuals who have volunteered to be selected for a variety of research projects. These panellists may of course choose at any time to withdraw from the panel and have their personal data removed.

EFAMRO and ESOMAR believe that both these concepts (of opposition and to be forgotten) are included in the current principle of data minimisation. The articulation of these rights would not change the current status for research, but should be expressed in such a way that they offer additional clarity to data controllers and data subjects on the lawful and fair processing of data.

24) Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

EFAMRO and ESOMAR support the clarification of the definitions of the terms used in the principles and the harmonisation of their application across the Member States. The process of harmonisation should however seek to understand current divergences in interpretation to ensure that no single national market or jurisdiction is disproportionally affected by a change in the application of the Data Protection Directive.

28) Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

"Transborder data flow" is a problematic concept with little practical application to the modern internet, distributed computing and global business organisations. EFAMRO and ESOMAR see this as a further reason to

strengthen and clarify the role of the data controller to ensure that they fully consider and address the protection and security of personal data before they elect how the data will be processed.

29) Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

The public and private sectors should operate under the same rules. Given that large scale public research, including the Eurobarometer depends on the expertise of private sector organisations, and that many European economies are depending on the private sector to stimulate future economic growth, such a differentiation would be unreasonable.

EMOTA

EMOTA Contribution to the Council of Europe Consultation on possible grounds for the Modernisation of Convention 108 on Data Protection

The European E-commerce and Mail Order Trade Association, EMOTA, welcomes the opportunity to participate in the Council of Europe consultation aimed at assessing whether or not the Convention on Data Protection (Convention 108) would need to be updated with regards to the use of new technologies and other market developments.

EMOTA represents 20 national associations in the European Union and beyond, which represent about 2600 traders (list of members in Annex). As the association representing e-commerce and distance selling in the European Union, data protection is a high priority for our members. In order to meet consumers' needs better, distance sellers use their data to improve service offerings and provide customer service. Free movement of data with a high level of protection for consumers' data is a prerequisite for unlocking the full potential of the single market, and especially for allowing small and medium sized enterprises to engage in cross border business.

General comments:

We would like to stress here that EMOTA and its members support this potential review as long as it is intended to help the development of the different online industries and to harmonise the rules on data protection in a greater area than strictly the geographical area of the European Union. We believe that the Convention and the Protocol have stood well the test of time and promoted a higher coherence among the Council Members. This endurance is the result of a responsible approach, based on a set of technology neutral principles and the conviction that a very detailed, issue oriented, approach would be detrimental to the development of, what was then, the future online economy.

Companies today need to be involved in the decision making process and in the past years, have taken their share of the responsibility (co-regulation and self-regulation). We feel that the European e-commerce industry took its role very seriously and together with other sectors have developed codes of conduct which tackle many of the issues mentioned in this position paper. Many of the data protection issues today come from a lack of education, and most importantly, from a lack of consistent enforcement. It has taken a very long time for Data Protection Authorities to take action towards coordination and cooperation, and many issues (such as data transfers, even within Europe) are still areas that are somewhat unclear and where companies have to face a long and bureaucratic process of negotiation.

You will find below our comments to the points relevant to EMOTA, as raised in the consultation document:

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

EMOTA and its members believe that the technologically neutral approach is the element that allowed the Convention 108, as well as the EU Data Protection Directive, to be future proof and encouraged the development of technologies and services in the European market and beyond. This is a precondition of any future proof regulation in this area. Technology evolves much too fast for a detailed regulation and

there is a real potential, as proven so far, for industries to be involved more in regulating the sector, either with the help of co-regulation or via self-regulation. Over regulation can and does stifle innovation which would be to the detriment commercial, consumer and economic interests.

For specific issues (such as social networks, behavioural advertising and profiling), authorities together with the industries can identify specific solutions either in the form of guidance, as illustrated by the Article 29 Working Party, the European Commission and relevant bodies in the Council of Europe, or self-regulation codes which can be adopted much faster, with greater efficiency.

*2. Should Convention 108 give a definition of the **right to data protection** and **privacy**?*

We support any approach which would lead to a higher degree of harmonisation in the broader European area. The European Union Data Protection Directive already includes a definition for data protection which was designed to be very broad. The right to privacy and data protection is included in the European Charter of Fundamental Rights (Article 8).

Any such initiative by the Council of Europe should be treated with great caution, as very often, when such discussions take place in parallel (in the context of the current review of the European Union Data Protection Framework) the end results can contradict and, or confuse existing frameworks , and this would be detrimental to the development of the online economy.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

EMOTA is supportive for an approach where authorities will take equally substantial commitments, as the industry has done already, towards a high level of protection for personal and sensitive data. EMOTA would support the continuation of the current comprehensive approach which has proven benefits to both business and consumers.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely **personal or household activity.** Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

We feel that the current wording covers well all scenarios if implemented correctly (WEB 2.0, or cloud computing). In the case of cloud computing and data stored on different servers, companies can use Binding Corporate Rules to ensure a high degree of protection for the personal data, which is a good safeguard for consumers as well. The need to introduce specific provisions on the data processed for purely personal reasons will, in practice, be impossible to verify and to enforce.

5. The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list? The definition of the **controller of the file** should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?

We believe that there is no need to create a specific provision on the collection of data. The current wording of Convention 108 is in line with the European Union Data Protection Directive. Secondly, the collection of data should not be regarded as an entirely separate process. The Article 29 Working Party has adopted a position already in 2010 regarding the various criteria that would determine if a party has acted as a controller or processor of data. We believe that a unitary approach would be very useful. We feel that the current European Union rules achieve this purpose and there isn't a real need for separate provisions. In the case of social networks specific measures can be adopted in cooperation with the main operators.

Protection principles

*7. New principles could be added to the Convention, such as the **proportionality** principle, which should apply to all operations carried out on the data. Such a principle is also linked to the **data minimisation principle** which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.*

EMOTA has shown support for the proportionality principle and there are a number of industry commitments already implemented in this area, next to the provisions of the Data Protection Directive and Regulation 45/2001. As new services and technologies are being developed, the inclusion of very specific provisions in the Convention, provisions that might go beyond the existing European Union framework, will result in a restriction of innovation, services and products being made available to consumers (geo-location, mobile applications).

*8. Should the question of **consent** be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?*

EMOTA promotes the collection and processing of data in a transparent way. Data are essential for a quality service that is relevant to the consumer. This is prerequisite of a modern and efficient online economy. We believe that in order to continue the relationship based on trust and respect, consumers need to be informed and given the choice. The only true form of consent (opt-out) is at the time of the collection, allowing the consumer to benefit from a maximum of transparency and choice before entering the contractual relationship.

Should the Convention make reference to "consent" such a provision should be very clear with regards to the possibility for consumers to opt-out and not require a "prior opt-in". Any other approach would undermine the fundamental way in which the online Environment is built and restrict severely the comfort and level of quality the consumer currently enjoys, including on mobile applications.

*9. Should the **legitimate processing** be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?*

EMOTA supports a unitary approach that enables both businesses and consumers to benefit from products and services in an area as large as possible. For this to be possible, legal certainty is essential. As more and more services are being developed, a general approach, such as in the European Union Data Protection Directive is essential.

*10. Convention 108 does not expressly mention **compatibility in relation to purpose**. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.*

We believe this aspect is in the European Union already very clearly regulated by the Data Protection Directive and Regulation 45/2001. As mentioned before, any platform specific concern should be treated in a separate context, together with that part of the industry.

*11. **Special categories of data** which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?*

Past discussions referred very often to the need to include other types of data in a specific list. We would like to stress here that current EU rules (Article 8, Data Protection Directive) are very clear with regards to the categories of data that are considered sensitive. Not all data should be considered

sensitive as this would severely limit choice for consumers and for companies (financial data used for the sale of insurance and other services or products for which a financial risk assessment is needed).

For example, in the case of some financial data (such as FRM – buying frequency and monetary value – the rate with which a consumer, anonymous, in a certain area, makes purchases, with what frequency and of what value), these are approximate indications that allow companies to better adjust their marketing campaign. These are data that cannot lead to any harm for the consumer.

Any extension of special provisions for certain categories of data should be preceded by a comprehensive impact assessment.

*13. Article 7 of the Convention addresses **security** in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of **data security breaches**?*

EMOTA is of the opinion that data subjects should be provided with transparency in the collection and processing of data. Generally we are supportive of consumers being informed of breaches of security in the case that they could be affected negatively by the effects of such a breach. However, there are many scenarios where such a breach would not have any significant effect. In many cases breaches are made public by the company already. And in most of the cases the data is encrypted. In the European Union context, controllers and processors are subject to strict provisions with regards to the security of data and in 2009 an obligation was introduced to inform consumers of breaches that might have a negative effect on their economic or social status. However, as mentioned before, the real problem is the enforcement of the rules and a data security breach notice would do very little to improve the subject's rights.

*14. There are special risks arising from the use of **traffic and localisation data** (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?*

Location and traffic data are essential tools for mobile e-commerce and related services. Current European Data Protection rules provide for a high level of protection for this category of data. The classification as sensitive data in the case of location and traffic data would significantly reduce the number of services available to consumers and limit drastically the potential of entire industry sectors.

*15. Should **accountability** mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?*

EMOTA believes that the sector is fully aware of its responsibilities and obligations. Within the context of the European Data Protection Directive, companies are already required to implement all necessary measures in order to the safeguard the data. Introducing new burdensome procedures for companies and regulators will have the opposite effect of that intended.

*16. Should the principle of **privacy by design**, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?*

We have to stress that the so called "privacy by design" principle would not be compatible with the technology neutral approach. Having specific requirements in an overall broad approach would reduce, in practice, the general applicability of this document. Privacy by design is a "toolkit" of measures designed to ensure that the use of data in a product or service is in line with the requirements of the Convention 108, or the Data Protection Directive. So far there hasn't been a clear definition of "privacy by design" and we feel that such a discussion would be welcome for the future.

Rights – Obligations
*18. The **right of opposition** is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.*

The European Union Data Protection Directive already sets a clear limit to how long companies can keep data in an identifiable form. All communications have to be based on the consent of the user. A right to oblivion is technologically and legally unrealistic. Companies need to first be able to recognise those subjects that have expressed their opposition to being contacted. Secondly, companies need to be able to refer to their own activity in order to improve and make future decisions. This is in all cases performed with data that no longer allows for identification.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

In our view, this already exists in the European Data Protection Directive and the e-Privacy Directive.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

The European Union Data Protection Directive already sets a clear limit to how long companies can keep data in an identifiable form. All communications have to be based on the consent of the user. A right to oblivion is technologically and legally unrealistic. Companies need to first be able to recognise those subjects that have expressed their opposition to being contacted. Secondly, companies need to be able to refer to their own activity in order to improve and make future decisions. This is in all cases performed with data that no longer allows for identification.

Sanctions and Remedies
23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

In a large number of countries subjects have already the right to join legal action. The referral to a collective redress system at this stage would only generate uncertainty.

Data protection applicable law
24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

In the context of the European Union, the 1995 data protection directive ensures a high, adequate level of protection for personal data, regardless of where the data are physically stored or where the data controller (or data processor) is established. We are worried that changing the current provisions on applicable law would contradict the underlying principle of the data protection framework, the principle of free movement of personal data.

Any changes to the above principles would certainly hamper the development of cross-border business, within the EU or in an EU-non-EU context. More specifically, changes to the current country-of-origin principle, whereby the law of the Member State where the controller is established is applicable, would create significant compliance costs for companies who own and operate (international) databases.

Data Protection Authorities
25. How to guarantee their independence and ensure an international cooperation between national authorities?

Within the different consultations conduction in the EU framework, all industry sectors stressed the fact that any lack of enforcement is the result of under equipped Data Protection Authorities. This view has been reflected on a number of occasions by the representatives of the Article 29 Working Party, especially in cross-border cases.

26. Should their role and tasks be specified?

Data Protection Authorities need to have a clearer role, tasks and resources to accomplish the responsibilities set by the European Data Protection Framework.

Transborder data flows

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

In today's online economy the free flow of data is essential, not only within the European Union, but internationally as well. Transfers of data within the same group of companies are still very complicated and expensive as a result of rules designed for a group of individual countries and not a single global market.

JOINT ENPA FAEP SUBMISSION ON THE REVIEW OF COUNCIL OF EUROPE CONVENTION 108 ON PERSONAL DATA PROTECTION

Introduction

ENPA, the European Newspaper Publishers Association and FAEP, the European Federation of Magazine Publishers welcome the opportunity to comment on the consultation concerning the modernisation of Convention 108.

ENPA and FAEP have not identified any specific problems with regard to the application of the current text of Convention 108. It is important, however, to underline, that in any amendment of the current Convention, the Council of Europe must find the right balance between the fundamental right of personal data protection and the fundamental right of freedom of expression. In the application and enforcement of fundamental rights, conflicts between these rights can arise.

As EU law recognises (Directive 95/46/EC), without any exemption of the press sector from personal data protection obligations such as prior data subject's consent for publication, there would be no free press and any press activity would be practically impossible to run. The inclusion of an exemption clause from obligations regarding the use and processing of certain personal data for journalistic purposes means that sound protection of personal data and privacy can go hand in hand with freedom of expression and freedom of press. Such an exemption is needed within any legal framework that aims to offer a reasonable balance of key fundamental rights.

Taking this dimension into account, the Council of Europe will need to ensure that the free and diverse quality press, which is an essential element of a truly democratic society, is properly safeguarded when reviewing the Convention on personal data protection. An approach coherent with the existing Directive 95/46/EC would be a sensible approach provided that both safeguard press freedom, by appropriate exemptions if need be.

It is fundamentally important to recognise that advertising is an important source of revenue for a free and independent press which is essential for any democracy. Any future Convention must therefore recognise the importance of advertising, which remains a crucial source of revenue for the press sector. Around 50% of printed press revenues come from advertising, whereas this is almost 100% in case of online press. In this sense overly restrictive and inflexible data protection rules impacting advertising, including online behavioural advertising, must be avoided as they would threaten the very existence of many publishers, in particular those who are developing online businesses and providing free-to-user content for consumers.

The importance of advertising for financing will even increase in future considering the growing shift towards the online press. Advertising must therefore be able to maintain the central role which it has for financing the press. Furthermore, it must be ensured that no new obligations which would rule out this possibility will be introduced by reference to data protection legislation. This is also particularly relevant to the possibilities of interest-based online advertising.

In a period where numbers of subscribers fall by up to 30% annually, due to both normal fluctuation, as well as the shift in readership from print to online, it is all the more important that magazines and newspapers are able to solicit new readers and subscribers under reasonable conditions. A press subscription is a product that must be explained and which has no retail outlet and which hence inevitably depends on personal and thus addressed contacts with potential readers. The right of recipients of advertising to decide on the use of their personal data can often be adequately reconciled with the legitimate interests of enterprises through information and the possibility to object. Many forms of advertising letters for press subscriptions are examples of such an area on which up to 20% of the subscription circulation of consumer publications can depend.

Questionnaire

Object and scope of the Convention, definitions

Technologically- neutral approach to be retained (Qn. 1)

Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

ENPA and FAEP would like to preserve the technology-neutral character of Convention 108. We believe that the protection of personal data is provided both at European and national level to a sufficient extent. The risk is that introducing restrictions will damage legitimate businesses and significantly reduce the ability of enterprises to develop sustainable business models, which would have unintended consequences for the European economy.

Many legitimate data processing procedures that are used for example in the context of online services constitute a valuable form of generating business and making relevant commercial offers for users.

The current regulations are formulated in a technology-neutral fashion and can be applied without undue complications to new data processing applications. A clarification or specification of the application of data protection rules to new technologies is therefore not necessary. The introduction of further requirements for data processing, not intended for the identification of a particular person, is not required.

A definition of the right to data protection and privacy (Qn. 2)

Should Convention 108 give a definition of the right to data protection and privacy?

Neither Convention 108 nor Directive 95/46/EC specify the right to data protection and privacy.

If any definition is introduced, then it must not entail any further restrictions of freedom of expression, including freedom of information, press freedom and freedom of commercial speech, nor enable any right of privacy and data protection to prevail over these fundamental rights. Nor should it introduce any stricter definition than currently exists, which could lead to legal uncertainty or further restrictions. In any event, the media will require appropriate exemptions

Protection principles

Problems of introducing data minimisation principle (Qn. 7)

New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Introducing a principle of data minimisation could pose serious problems for independent publishing, if it meant that journalists would be prevented from producing well-researched, quality articles due to limitations and restraints being imposed on the data they could use. The press sector has a specific role in a healthy democracy, delivering news independently from the state power. In this role it has to be able to provide properly-researched information and must be free to be able to gather and publish any personal data relevant for editorial reporting as well as protect its sources. Newspaper and periodical press publishers should therefore be entirely free to gather and retain personal data in the course of the work of journalism (and broader artistic and literary activities) in line with its own appreciation of which personal data are necessary or relevant.

Editorial freedom of the press is not possible without any exceptions to data protection law. In the same way as Directive 95/46/EC includes an exemption from certain data protection rules for journalistic purposes, it is vital that this is reflected in Convention 108. The result of not doing so would jeopardise the fundamental right of freedom of expression, the provision of quality journalism and media diversity. A free and independent press is an essential condition for a functioning democracy and must be reinforced in any new legislation.

Question of Consent (Qn. 8)

Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Media exemptions would be necessary to any question of consent whether in respect of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing.

Any proposed changes should avoid any obstacles that would hinder journalists from providing quality content (e.g., archiving articles as well as research material for preparation of articles or day to day newsgathering, investigation, checking, editing, deleting, whether or not leading to publication of material, as well as publication and further dissemination of material).

Also with regard to advertising, being the lifeblood revenue for the entire press sector, with a stake of practically 100% for online content, and free newspapers, no new or more onerous obligations of consent should be introduced.

As regards advertisements based on online preferences, voluntary self-regulatory initiatives are preferred and we believe such an approach is more beneficial to all parties involved than any further restrictive legislative intervention in this field.

Compatibility in relation to purpose (Qn. 10)

Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

See answer to Question 7.

Special categories of data (Qn. 11)

Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

A free and independent press has to be able to report on issues in an objective way by using certain categories of personal data, even if those data are considered as sensitive (as under Directive 95/46/EC). The current rules on processing of specific categories of sensitive data as laid down in Article 8 of Directive 95/46/EC fall under the general exemption clause for publishing houses set out in Article 9 of that Directive.

This is the only logical solution to safeguard a free and independent press. For example, without comprehensive journalistic exemptions, it would be impossible for media organisations even to cover public events, from political meetings to religious services to industrial disputes or demonstrations (perhaps relating and involving participants in ways which would identify them and their political, medical, trade union, religious etc beliefs) or accidents or health and safety issues or acts of sectarian violence or terrorism, featuring identifiable perpetrators or victims or bystanders.

The objective reporting on such events is thus severely undermined if the account would be subject to censorship by the data subject, invoking in this case any kind of convictions or references to the person or organisation reported on as falling under sensitive data. Media organisations' ability to report crime, criminal investigation, the progress of criminal and civil cases and court or tribunal proceedings, civil and criminal or making reference to them could be severely impaired. In the case of news provision, the right of access to information and freedom of expression and press freedom should prevail over the protection of sensitive data.

Specific protection to certain categories e.g. children (Qn. 12)

A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

Concerning the possible introduction of specific obligations for data controllers on the type of information to be provided and on the modalities for providing it, including in relation to children, we believe that these are not necessary. Media literacy and education are useful and efficient tools to increase minors' awareness of the positive and negative effects of the Internet. Parental control and education in schools also have an important role to play. In this context we support the promotion of efficient awareness-raising.

Accountability mechanisms (Qn. 15)

Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

We strongly support voluntary self-regulation and see it as an effective tool to ensure an effective application and implementation of the current data protection framework.

Furthermore, ENPA and FAEP are strongly of the opinion that the criminalisation of breach of data protection, especially by the press, has serious consequences for press freedom and freedom of expression. This can for instance be the case with overly general descriptions of illegal acts or omissions bearing the risk of a broad interpretation, as discussed currently in the context of the Hungarian media law.

Newspaper and magazine publishers share the view that rather than implementing stricter legislation or increasing the powers of regulators, proper enforcement of the current rules is the most appropriate solution to counter many of the current concerns. Violation of national rules and abuses of personal data have not remained unsanctioned because of a lack of legislation but rather because of ineffective enforcement.

Concerning the enhancement of the role of national Data Protection Authorities (DPAs), it is important that these authorities have sufficient financial means, human resources, political independence and adequate training to efficiently carry out their current tasks at national level.

Privacy by Design (Qn. 16)

Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

In reference to the concrete implementation of the concept of 'Privacy by Design', we do not believe that subjective opinions on how privacy settings should look should be imposed on consumers. This is neither necessary to guarantee that consumers have sufficient control over the use of their personal data, nor feasible with regard to the huge variety of information and communication systems and technologies. If users are educated about privacy risks and data management in general, as well as about specific practices and policies for safer internet use, and empowered to implement their privacy preferences they are able to make their own informed choice.

Rights - Obligations

Right of access (Qn. 17)

The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

We are of the view that any move towards a property right over individuals' personal data would have far reaching consequences which go way beyond the objective of controlling personal data. (Clear and precise conditions for the processing of personal data are already laid down in Directive 95/46/EC). The introduction of a "property right" over individual personal data would not solve problems that have arisen in the online environment as many of the discussed cases concern data protection breaches that are already forbidden under current data protection rules. It would instead have major implications on freedom of expression, freedom of information, press freedom and the day-to-day business of companies.

Right of opposition (Qn. 18) and right to remain anonymous (Qn. 21)

The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

Should everyone have a right to remain anonymous when using information and communication technologies?

In relation to the so-called "right to be forgotten" (or "oblivion"), it is unnecessary to introduce such a right into the legal framework (Directive 95/46/EC provides an efficient means for the data subject to object to the processing of their personal data). While we understand that consumers may want to retrieve photos etc. from social networking sites, introducing a "right to be forgotten" would have devastating consequences for publishers and freedom of expression if it resulted in a "right to erase". We therefore ask for all possible guarantees to avoid this.

In the first place any applicable right to be forgotten would be detrimental for maintenance of extensive news archives and press libraries. They form an important and indispensable resource for high-quality news content, as well as being an important source of historical information.

Background and unpublished information may also have to be retained for legal reasons, in order to provide a defence in the event of a complaint. Journalists therefore need to be allowed to continue retaining what is technically "personal data" in archives. A press which is independent from state influence is essential for a healthy democracy based on an informed and critical civic society. Any interference in this matter bears the risk that archives - and history itself – could be censored.

In the second place, it should be borne in mind that retaining personal data for marketing purposes is of high importance for the continued existence of a healthy press sector, as without this it is much more difficult to maintain readership.

Sanctions and Remedies

Class actions (Qn. 23)

Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

Class actions are not an appropriate way forward for various reasons. For example such actions, especially when politically motivated, could pose a serious threat to publishers including as regards the potential harm to freedom of expression.

Data protection applicable law

Applicable law (Qn. 24)

Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

We would be concerned about any revision of the provisions on applicable law which actually resulted in Member States regimes imposing greater burdens upon business. Also we are concerned that more restrictive rules under other countries' laws may encourage legal proceedings to be brought against media or otherwise inhibit press freedom in the country of origin of these media companies.

Data Protection Authorities

Data Protection Authorities (Qn. 25)

How to guarantee their independence and ensure an international cooperation between national authorities?

ENPA and FAEP believe it is key that DPAs have sufficient financial means, human resources, political independence and adequate training to efficiently carry out their current tasks at national level.

EUROPEAN PRIVACY ASSOCIATION

Introduction

As the Council of Europe celebrates its 30th anniversary, we are also reminded that there are new data protection challenges each and every day. EPA is encouraged that the Council of Europe is engaging in a process of revising its Data Protection Convention (Convention 108) to meet and overcome these challenges. This is an extremely important issue.

EPA pursues a pan-European approach. The contribution that follows reflects the ideas and thoughts of several European fellows that deal everyday with privacy and data protection issues in their capacity as privacy experts in academia, law and business.

EPA aims to represent the voices of various European stakeholders engaged with privacy in different cultural, economic and social contexts around Europe. We are delighted to work with **The Italian Institute for Privacy** (Istituto Italiano Privacy - **IIP**) and the **Spanish Privacy Professional Association** (Asociación Profesional Española de Privacidad – **APEP**) who also contributed to this submission.

EPA wishes to thank all individuals and organizations that have provided ideas and thoughts to this contribution and for the support they bring to the work of our association every day.

European Privacy Association (EPA)

Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

A technologically neutral approach is probably the best approach in order to ensure that the Convention is general enough to be applied to most of the possible situations – and also to be adapted for technological changes. Generality and simplicity should be kept as reference points for the new version of the Convention. Of course, considerations arising from existing technologies may – and should – be kept into account but with the aim to elaborate general rules that may be applied today and in the future.

Should Convention 108 give a definition of the right to data protection and privacy?

The right to data protection and right to privacy should be defined at the global level; consistency is key in order to ensure and enforce these rules since we live in a global world. In the revision of Convention 108, it would be extremely useful to work towards a widely recognized definition of the right to privacy and the right to data protection, which should take into consideration not only EU definitions (e.g., Arts.7 and 8 of the Charter of Fundamental Rights of the European Union) but also the ones of other countries, continents and legal traditions.

Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes, the violation of citizens' data protection rights by public authorities should be contemplated by the Convention.

Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

Specific rules for a "natural person" processing personal data for purely personal or household activities should be established. Web 2.0 has exponentially increased the number of situations in which natural persons misuse personal data and create significant damage to other natural or legal persons. On the other hand, natural persons processing personal data, in the course of purely personal activity, may not be subject to disproportionate duties and obligations, e.g., data security (Art. 7) or Transborder Data Flows (Art. 12).

The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list? The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file? New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

The collection of data should be included in the definition of automatic processing; the list of operations could even be extended to those contemplated by Art. 2, b, of the EU Data Protection Directive 95/46/EC. New technologies, including cloud computing, are significantly challenging the soundness of definitions of roles, such as "controller" and "processor". It is foreseeable to see more and more technologies, which enable automatic data processing to be carried out by multiple players. It is important not to define their names and roles but rather their processing activities, relevant duties and obligations, and related liabilities.

New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

The Convention already includes the proportionality and data minimization principle as a key point in data protection under Art. 5 – Quality of data. From this point of view, revising Article 5 of the Convention is not necessary.

Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

No, it is neither a workable solution to always mandate prior data subject consent, nor it is a guarantee of fair and lawful processing – especially regarding automatic processing. Users very often opt-in without even knowing to what they are opting-in.

Clear and transparent information is key for the data subject to determine whether or not to allow the relevant processing (not necessarily by way of opt-in but also by opting-out). The principle to elaborate on is that of clear (easy to find and understand) information and transparency on data processing.

Given clear information and transparency on data processing, prior consent may be mandated only for specific data processing.

Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

An alignment of the Convention with the Directive 95/46/EC seems useful. The list of legitimate grounds for data processing may eventually be based on Directive 95/46/EC, leaving the possibility for the Signatory Parties to recognize further legitimate grounds as long as they are not incompatible with the general rules and principles of the Convention.

Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Article 5, b, of the Convention already states that personal data shall be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes". The main issue is not mentioning the compatibility in relation to purpose but rather to extend the application of the aforementioned provision to any processing of personal data. The text of Article 6, 1, b of Directive 95/46 should be used as model.

Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

The content of Article 6 is well balanced and we do not see a significant risk of excessive application of the restrictive regime. However, we recommend establishing a global definition for sensitive data (e.g., trade union affiliations fall under the definition of sensitive data in the Directive 95/46/EC; whereas they do not according to Art. 6 of the Convention). Regarding biological and biometric data, provided that they may reveal health life, they fall under the existing restrictive regime. As pointed out above, the Convention should be kept as general as possible and

contemplate the protected values (such as health life) rather than focusing on specific kinds of personal data.

A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

As far as automatic processing is concerned, it is not sustainable to have specific provisions for processing children's data without setting forth a more general obligation for users to identify themselves on the Internet (e.g., by means of a e-ID or strong e-signature). At this point in time, we believe that the Convention should set forth adequate protective rules, which cover both adults and children.

Protecting children online should be pursued by setting forth an ample set of coordinated provisions - specific data protection rules being one of them.

Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Data security breach notification already exists as an obligation in the US. It is set forth in the EU Directive 2009/136/EC, which is soon to be implemented in the Member States.

Data security breach notification should be governed globally by clear rules outlining when notification should be given, to whom and in which way.

There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

First, traffic and localization data are not always personal data. If they are personal data, they will be processed accordingly or more restrictively in case they fall under a special category of data.

EPA believes that the Convention should be focused on the protected value (privacy) rather than on the specific kinds of personal data and specific means of collecting personal data.

Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Accountability mechanisms should be created to foster data protection; they should be clearly defined, not excessive, and implemented the same way among the signatories. Incentives should be created for implementing accountability mechanisms.

Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Privacy by design should be promoted. However, we think it should not become a legal obligation or a legal principle. The aim of the Convention is to provide rules and principles that are implemented by the industry according to the modalities they prefer. The goal is that privacy and data protection are eventually respected, this could in fact be achieved by the design of a technology or by the way or mechanism it is used or deployed.

The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

The right of access will align the Convention with what was set forth in the Directive 95/46/EC.

Transparency in the processing must be guaranteed. However, automatic processing and its logic are becoming more and more complex, involving a significant number of players. We have some doubts that such an obligation would be sustainable without bearing excessive costs.

The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

We believe the right of opposition and the right of oblivion are two different rights, which are not directly related. Therefore they should be addressed separately.

Moreover, we have some doubts that the right of oblivion can be exercised on the Internet without breaching other rights and freedoms (e.g., freedom of press or freedom of expression).

Should there be a right to guarantee the confidentiality and integrity of information systems?

Yes, there should be a right to guarantee the confidentiality and integrity of personal data.

Should a right 'not to be tracked' (RFID tags) be introduced?

We believe that instead of a right 'not to be tracked', there should be an option for the data subjects 'not to be tracked'. Data subjects should be informed about tracking practices and contextually provided with the option and technological means in order not to be tracked in a transparent manner.

Should everyone have a right to remain anonymous when using information and communication technologies?

A generic right to be absolutely anonymous when using ICT means – in the sense that it is not possible for anyone to keep track for instance of the Internet connections made by a user, of the websites visited, etc. – cannot be accepted or implemented. In practice, citizens need information about their use of ICT means (e.g. to contest the invoice for the use of services) and very often the data, which are necessary in the framework of criminal investigations.

On the other hand, we believe that data not be used for illicit purposes and not disclosed, unless in specific cases set forth by law. The Convention, together with the European legislation, already prevents these abuses from happening.

Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

The link between right to data protection and freedom of expression is pivotal and should be carefully addressed by the Convention – starting from the assumption that the freedom of expression is a basic right that can be balanced and limited only in specific cases when other important values, such as person's dignity, are in danger. Therefore, a 'link' with the provision about freedom of expression in the European Human Rights Convention in the recitals of the Data

Protection Convention should be addressed (e.g.: "Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing and taking account of the fundamental value of the freedom of expression as recognized by Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms [...]".)

Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

The possibility to introduce class actions in the field of data protection law could be taken into account, provided that the class actions are intended to protect consumers and do not become tools to eliminate competitors. The Convention is not the best organization to introduce the class actions since it is aimed to be a general legal instrument; other European laws are probably better to eventually encompass class actions.

The same considerations as above apply to alternative dispute resolution mechanisms.

Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Yes, a rule determining the applicable law to the data processing should be considered in line with the provision of Article 4 of Directive 95/46/EC. In practice a rule such as that of Article 4 of the Directive implies that each Signatory State has more or less the same level of data protection guarantees or, in different terms, a high level of mutual trust among the Signatory Parties. The end goal is that data protection rules of the Signatory States are equivalent; and thus the 'controller' by complying with the rule of the State where it has the main establishment it can lawfully process data also in its branches located in other Signatory States.

How to guarantee their independence and ensure an international cooperation between national authorities?

The issue of independence of data protection authorities should be left to the national legislation of the Signatory Parties, taking into account their particularities. In general terms, the existing provisions of the Convention together with the Protocol are fairly balanced.

Should their role and tasks be specified?

Yes, their role and tasks should be specified; in addition, their decisions should be recognized in other Signatory States.

The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

We agree.

Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

This issue is very important and must be carefully addressed. The notion of "transborder data

flows" cannot be neglected, due to the importance and business impacts of technologies such as cloud computing. In this sense, internationally agreed minimum rules are necessary. Regarding their content, it would be pivotal to avoid the applicability of several national laws in case of "transborder data flows" involving several countries. The applicable data protection law should be that of the country where the most important part of the processing takes place or, in case this is not possible to be assessed, the place where the data controller is located. The current means to regulate transborder data flow (outside the EEA) set forth by the Directive 95/46/EC fall short when applied to the cloud computing environment, which is characterized by multiple transfers often by several parties. The Convention could try to devise new means to support complex transborder data flows.

Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

The basic principles should be the followed by both the private and public sectors. BCR should be streamlined and the relevant procedure simplified before they can take off in the private sector.

Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

The primary function and goal of the committee should be setting global standards.

APEP Contribution

Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

The law is always a step behind technology. Therefore, a technologically neutral approach must be privileged. Further, although Convention 108 does not provide an answer to every data protection or privacy issue (and cannot be expect to be able to do so), it has proved to be useful because it is general and simple. This approach should be maintained.

Should Convention 108 give a definition of the right to data protection and privacy?

Yes. Both definitions are necessary. Personal data may be private or not. Personal data and privacy are different rights (even if they may occasionally be related) and require a different regime.

Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

A fundamental right has always been created (at least in Europe) against public authorities. However, protection would be incomplete if damages that might be caused by others (companies, social media, other data subjects, etc.) are not also contemplated.

Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

The regulation on privacy is sufficient to address violations caused by users.

However, this is not the case for data protection infringements. An exception to the current data protection regime for personal or household activities will be useless and counterproductive if not accompanied by a specific regime. The regulation must sanction users that cause damages by misusing personal data -whether private or not- of others (friends, children, relatives, etc.). However, it would be disproportionate to impose on users obligations such as to register databases, to provide information along the lines of Articles 10 and 11 of Directive 95/46/EC, to implement security measures (or to ensure that they have been implemented, for example, by the relevant platform used for the upload or tag of images or for any other data processing such as social networks), etc.

The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

Collection must be included in the concept of processing, irrespective of whether it is automated or not.

The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

The concept of controller of a processing (is still the file a useful concept?) must be reviewed to include the one/those which has/have *de facto* the right to decide on the personal data processing purposes and means, either by operation of law or by virtue of contractual arrangements with the data subject or with third parties.

For legal certainty purposes, it is important to specify that the controller should have its own legal

personality. This is especially relevant in order to properly claim a liability or to avoid nonsense situations such as "processing agreements" between a branch and its "parent company", both sharing the same legal personality.

There could be several controllers regarding a file or a processing. Different persons may decide to process the same data (included in a single file or in different copies of the same file), for the same purposes (joint controllers) or for different purposes (several controllers).

New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

A definition of processor is useful. If the definition of the Directive 95/46/EC is reproduced, it must be clarified whether or not the use of a processor is a processing "means" or "equipment" of the controller that contracts such a processor.

The definition of the manufacturer of technical equipment used for personal data processing might be useful if linked to a "privacy by design" obligation. However, the proper implementation of the "privacy by design" concept or the PIA (privacy impact assessment) primarily requires the controller's involvement since it alone decides on the actual processing purposes.

New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Yes, absolutely.

Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

To inform the data subject of the processing circumstances must be a general rule in order to ensure transparency.

Nevertheless, free consent must be considered not as a necessary condition to any fair and lawful processing but as one of the legitimate grounds (among others to be defined) on which the controller must rely.

Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

Convention 108 should, at least, not contradict Directive 95/46/EC (in particular, the "legitimate interests" ground set out in Article art. 7 f).

Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

We see no need to mention the compatibility concept, unless further guidance is provided in order to ensure the legitimacy of a "secondary use". However, this will be contrary to the goal of keeping the Convention general and simple.

In Spain, referring expressly to the compatibility concept has proved to be more problematic than the issues that it aimed to solve since it has been -mistakenly- construed as "different". Further, it adds very little to the proper way of construing the scope of the legitimate purpose(s) since any

fundamental right must be construed narrowly.

Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

As a general rule, special categories of data are the core of private data (as opposed to other personal data) and deserve a specific and more stringent regime. However, the damages that might be caused by processing these sensitive data (to privacy) depend on the processing purposes. For example, normally, the processing of illness records, pregnancy leaves or trade union membership by an employer for HR purposes or in accordance with legal duties should not be treated the same way as the sale of genetic data for commercial purposes.

We do not share the opinion that the definition of personal data enables the inclusion therein of any governmental identifier in all countries, all biological data, all biometric data, all vehicle plates, all cell numbers, all IP addresses, etc. and, even less, for any possible controller. Not everything that could be potentially associated to someone anywhere in the world must be included *per se* in the category of personal data and data protection regulations do not solve all problems involving individuals. The consequences of "labeling" as personal data are extremely burdensome for controllers and have an impact on their ability to contribute to the creation of employment and economic growth and welfare in the EU.

Having said this, (i) it is difficult to support that any (national) identification number is sensitive; (ii) we fully agree in including those biological or genetic data in the "special categories of data" *provided that* they are *also* personal data; and (iii) we would be more cautious regarding biometric data (which is a broad concept including a wide variety of information), since not all of them or not any processing of them reveal health-related data.

A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

There is no debate as to whether children deserve specific protection. There is, however, a debate, as to what the relevant age is (13?, 14?, 18?), whether and when the parental control invades the children's right to privacy, who must grant the parental consent (only one parent or both) and how a controller may reasonably ascertain who is legitimized to grant the consent (again, one parent, both, another guardian ...), how easy it is to provide a false identity online, etc.

Obviously, data protection regulations are not and cannot be the sole tool to provide protection to children. In any event, the protection that could be offered would only be useful if the duties imposed on controllers can be reasonably achieved by them in terms of effective control and cost. Further, compatibility with the minimisation principle must also be ensured.

Three thoughts: (i) specific duties should be imposed when children are the target of the processing; (ii) the regime must be based on a duty of diligence to be measured through a PIA, and not a duty of obtaining a result; and (ii) it would help to have a digital identifier that enables identifying the age of the data subject or an advanced electronic signature as a duty imposed on all citizens with legal capacity to contract.

Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

The question is whether this notification ensures effective protection. In a global economy and

society, risks are universal and the remedies must in turn be universal. If a security breach notification is imposed (note that Directive 2009/136/EC has not yet been implemented), the internal market must ensure that all items are regulated the same way within the EU: who must notify (only telecom operators, other sectors, all controllers?), when the notification must be served (triggering event(s) and deadline), how (communication means, in view of the costs involved) and whether the DPA must also be notified. Europe must avoid having as many data security breaches regimes as number of States.

There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Not all traffic and localisation data are personal data. The fact that they can reveal this kind of sensitive data does not entail that they actually reveal them since this requires matching this information with other (publicly available or not) information.

In any event, if they happen to be linked to personal data, general rules on the processing of special categories of data would apply.

If they are not (yet) personal data, the special regime would be linked to privacy and not to data protection matters. A "do not track" privacy regime could be envisaged as well as with respect to other information that cannot and should not be considered personal data in all circumstances (such as IP addresses or information collected through RFID, cookies or other similar tracking devices).

Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Yes. In this respect, for accountability to produce effective protection, both qualified persons (certified) and a budget (i.e., effective decision power within an organisation) are required. There should also be a "reward" (e.g., a sanction reduction) for "accountable" controllers and the processors in the event that the data protection infringement is only due to an exceptional error.

Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Absolutely, privacy by design and PIA are indispensable to ensure effective protection.

The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

We are uncertain that this would make the protection more effective but it will certainly entail more work for controllers which will prove complex and costly to implement. In any event, knowing the logic of processing is more linked to avoiding the creation of a society that is based on decisions adopted without human intervention (see Article 15 of Directive 95/46/EC).

In any event, the limits of the right of access must be clarified because it is widely used to circumvent, for instance, the right to access administrative files, which is subject to other rules. The right of access in data protection needs to be protective and reasonable; it should not entail the right to access any data on the data subject included in any document, back-up copy, etc.

The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

The right to oblivion is not a subcategory of the right of opposition. It goes beyond stopping a specific processing since it has retroactive effects. Therefore, the question here is whether individuals must be responsible for their past actions *sine die* and whether it is reasonable that they have the right to "rewrite" their past and thus also the past of others.

In addition, for any right of oblivion to work, in particular, in the *online* environment, the source of the publicly available information must be involved and privacy by design must be an obligation to be imposed on social media, official gazettes, public registries, etc. Data protection (as is the case for privacy or other fundamental rights) is not absolute: striking a balance between interests would be necessary to determine which fundamental right or freedom must prevail on a case-by-case basis.

Should there be a right to guarantee the confidentiality and integrity of information systems?

Not all the information stored in IT systems is personal data. In any event, it is necessary to ensure the confidentiality and integrity of personal data irrespective of where they are stored. An automated processing environment may help to build categories of specific security measures to be implemented (authentication, back-up copies, encryption, etc.). A cost analysis would also have to be carried out, particularly regarding certain sectors which may have specific mandatory security measures (irrespective of whether or not the information is personal data) such as the financial or health sectors.

Should a right 'not to be tracked' (RFID tags) be introduced?

Yes, as an option to be made available to the data subject (privacy by design) but not as a prohibition. This concept may apply to other tracking devices that do not necessarily collect personal data but other information that may ultimately also harm privacy, such as cookies.

Tracking devices or technology are not bad *per se* but certain uses must be limited when privacy is to prevail over other interests (PIA). For instance, tracking Alzheimer patients or lost luggage, vehicles, children or pets should not be prevented.

Should everyone have a right to remain anonymous when using information and communication technologies?

Not always, especially if the anonymity is used to commit a contractual breach or an offense. For example, an employer must be able to monitor any employee's action for which it may be held liable (e.g., in view of leniency anti-trust proceedings or in order to honour contractual or legal obligations) and to protect its legitimate rights (e.g., confidential information, IP rights, security of its own IT systems or compliance with security measures on personal data protection).

Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

Yes, but this requires a case-by-case analysis. Any regulation in this regard must ensure flexibility: it must provide guidance criteria but not a predetermined and general evaluation.

Should class actions be introduced in the Convention? Should more scope be given to

alternative dispute resolution mechanisms?

No, this would only increase the tortuous use of the data protection and privacy regulations by data subjects (e.g., employees or unsatisfied clients), trade unions or competitors.

Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Only if the criteria enables effective protection under one EU regime (not contradictory to Directive 95/46/EC) and does not entail a competitive economic disadvantage for the internal market.

In this regard, the use of the concept of "processing means" for controllers established outside the EU contained in the Directive 95/46/EC must be reviewed and replaced by the market (residence of the data subjects) targeted by the controller, in accordance with the criteria used by the related regulations, such as those on e-commerce/information society services and consumers.

Further, data protection regulations within Europe must be deemed equivalent for all purposes, not only for international data transfers. For instance, the security measures that are compliant with French data protection regulations must be deemed equivalent to those applicable in Spain or the processing for the compliance of a legal duty imposed by a German law on the Spanish controller must be deemed equivalent to the one carried out for fulfilling a legal duty imposed by Spanish law.

How to guarantee their independence and ensure an international cooperation between national authorities?

Separate budget and no hierarchical dependence on the government (see the appeal before the ECJ against Austria (C-614/10)). International cooperation between national authorities must be imposed (not only encouraged) for global issues.

Should their role and tasks be specified?

Yes. A mutual recognition system would also be welcome, in particular, regarding BCR.

The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

The "adequate level of protection" determined by the EC Commission or the supervisory authorities (but not by the data controller or the data processor) according to Directive 95/46/EC has proved useful. It would be advisable for Convention 108 to expressly recognize the decisions on "adequacy" issued by the EC Commission according to Article 26 of Directive 95/46/EC.

The analysis of the "adequate level of protection" standard has, to date, mainly focused on countries and certain territories. The same analysis on sectors and contractual systems should also be encouraged:

(i) specific sectors (as has been the case to a certain extent, regarding PNR), such as health or financial sectors which are heavily regulated to ensure the confidentiality and integrity of the information (personal or not); and

(ii) "contractual systems" (as has been the case for EC standard contractual clauses), such as the BCR, which requires a legal recognition and a clear regulation on how the external binding nature is gathered.

Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish

internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

This is the aim of the "Madrid Resolution" (issued at the 31st International Conference of Data Protection and Privacy) but it cannot be achieved if its principles are not incorporated in a legally enforceable document (such as the Convention). This will not solve all the issues, but it is certainly a start.

Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

Both sectors must share the same principles, but it is true that each sector has different "data protection" needs and creates different risks.

In any event, for the moment, BCR (which is mainly based on the accountability principle) seems to be more necessary for the private sector. However, accountability is also indispensable (arguably even more so) for the public sector.

Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

Standard setting seems to be the most important function. Its cooperation with the Article 29 Working Party and the EDPS must be ensured to avoid inconsistencies since they have a significant impact on the development of the internal market.

FEDMA

FEDERATION OF EUROPEAN DIRECTAND INTERACTIVE MARKETING

PUBLIC AFFAIRS & SELF-REGULATION 10 March 2011

Modernisation of the Council of Europe Convention 108
FEDMA submission

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

The Convention 108 should remain technologically neutral in order to keep enough flexibility towards the development of new technologies. A more detailed text could lead to a situation where new technologies would not be covered when they arise, and constant changes would be necessary to match the evolution of technologies. The current wording of the Convention 108, based on principles, makes this instrument "future proof" and therefore provides better protection. The practical use of innovative technological concepts, such as aggregated data, cloud computing, IP-Addresses, RFID, cookies, and geo data must and can be solved within the existing framework of the Convention's technological neutral approach.

2. Should Convention 108 give a definition of the **right to data protection** and **privacy**?

The right to data protection became a fundamental right in the Lisbon Treaty of 2007. Article 16 of the Treaty on the Functioning of the European Union† lays down a specific and comprehensive legal basis, which is now prominently placed in Title II on "Provisions of general application". The substantive parts of this provision clearly affirm that "Everyone has the right to the protection of personal data concerning him or her" (paragraph 1) and that compliance with data protection rules shall be subject to the control of independent authorities (paragraph 2). We therefore believe that Convention 108 should not give a definition of Data Protection.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

We strongly believe that this approach should be maintained. Both industry and governments should abide by the same rules. Especially when one considers that governments generally collect and process large amounts of sensitive data (income, health, criminal record) en have the means to interconnect these databases. This principle also applies to law enforcement. These days law enforcement often uses governmental data such as tax returns to track suspects. They therefore should also abide by the same rules.

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

5. The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The collection of data is already included in the Convention, in article 5 (a) which specifies that "personal data undergoing automatic processing shall be obtained and processed fairly and lawfully". Thus, the collection of data does not require special provisions.

The definition of the **controller of the file** should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

Defining several criteria as part of a definition brings a certain danger as it becomes difficult for organisations to determine whether or not they fall within the definition. This becomes even more of a problem if the criteria are cumulative. As an example, there can be several joint data controllers for one file of information, particularly if the data is pooled and used by several data controllers.

6. New definitions may be necessary, such as for the **processor** or the **manufacturer of technical equipment**.

A new definition for a processor may be necessary and should be along similar lines to the one included in the European Data Protection Directive. However, we wonder how defining new parties, such as a definition of the manufacturer of technical equipment, would improve the convention.

7. New principles could be added to the Convention, such as the **proportionality** principle, which should apply to all operations carried out on the data. Such a principle is also linked to the **data minimisation principle** which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

A proportionality principle is not required as under Article 5a of the Convention personal data must be obtained fairly and lawfully. A data minimisation principle is not required as under Article 5b personal data can only be stored for specified and legitimate purposes and not used in a way incompatible with these purposes and under Article 5c must be adequate, relevant and not excessive in relation to the purposes for which they are stored.

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

8. Should the question of **consent** be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

We believe that the principle of transparency is key in the processing of personal data, and consider the obligation to inform as a intertwined part of this principle. It is important to set up a clear ground for the processing of personal data. As defined in the 95/46 Directive, consent is one of the criteria for making data processing legitimate. Data processing is also allowed when it is necessary for the purposes of the legitimate interests pursued by the controller. This is a legitimate ground for data processing, provided that the consumer is well informed. Making consent obligatory for all data processing would be a disproportional burden for organizations. And it will not benefit the consumer, because it will influence the competitiveness of markets. If new companies cannot get in contact with their potential clients, this will strengthen the hegemony of the large market players.

9. Should the **legitimate processing** be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

We do not see why the convention should repeat the Directive 95-46 grounds for legitimate data processing. It is our strong belief that these provisions should be part of a directive and not a convention. A parliamentary process (bottom-up), in line with the most fundamental principles of democracy allows for a application of the proportionality principle. These should not be subject to the content of a convention.

10. Convention 108 does not expressly mention **compatibility in relation to purpose**. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Although the Convention does not mention compatibility in relation to purposes, it does mention incompatible in relation to purposes in Article 5b. The point here is that individuals need to be told if their personal information is going to be used in ways which they would not expect it to be used. For example if one request a brochure from a travel company, it is reasonable to assume that personal details may be passed on to another organisation to send the brochure to me.

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

11. **Special categories of data** which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

We believe that the current categories of "special categories of data" should not be extended to cover the categories listed above. Biometric and genetic data will in certain cases be classified as "special categories of data" under the Convention if they relate to a person physical or mental health or conditions or his sexual life. A person's family history may also be a special category of data under the same grounds. We do not believe there is a need for minors, data to be treated as a special category of personal data. Minors' personal data is already fully protected under the Convention. If it was made a special category of personal data there would be problems, particularly in the online world of a parent/guardian giving express consent for any processing of the data.

12. A specific protection could also be applied to certain categories of data subjects. In particular, **children** may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

In this context, parents should be reminded, aided and held accountable for their children's exposure and education towards a responsible use of the internet. In all member States of the Council of Europe, it is the custodian's role to supervise and foster children. In parallel, schools and play-schools should cover the risks of internet usage in their curricula.

13. Article 7 of the Convention addresses **security** in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of **data security breaches**?

We understand that security of data is one of the utmost importances. Data must be protected against unauthorized access and a data subject should be able to trust that his data is secured by a controller. Therefore we are sympathetic to this concept, because it is an incentive to secure personal data. But we believe that a Breach Notification is an elaboration of the principle of protection against loss. We believe this elaboration should be addressed in a directive, because it implies a lot of obligations which constitute a breach notification. What are the obligations? Is there going to be a differentiation between organizations with a small database and a large database or are there any other criteria to be developed? These specifics should be addressed in a Directive, not a Convention.

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

14. There are special risks arising from the use of **traffic and localisation data** (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Traffic and location data should only be processed for marketing purposes or in connection with value added services with the consent of the subscriber. Moreover, the use of geo data must be solved within the existing framework of the Convention's technological neutral approach. Each new technological development can´t be covered by specific amendments to the conventions of the Council of Europe, as the revised law would possibly become obsolete as soon as technology or its use changes. A technology-neutral approach has the benefits to allow for innovation. Self-regulation has proven successful dealing with sector specific technical or legal issues that are challenging or need clarification.

FEDMA is the only European Trade Organization that has two Codes of Conduct – on the collection of personal data for direct marketing and online marketing -approved by the Article 29 Working Party. These Codes provide clear and unambiguous rules, telling organization how to implement privacy principles in their organizational marketing processes. However, if technique based legislation is approved, this self regulation will no longer be applicable.

15. Should **accountability** mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Organisations already have to comply with the national data protection laws in states which are signatories to the Convention. Introducing an obligation to demonstrate compliance could be a burden, particularly for SMEs.

16. Should the principle of **privacy by design**, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

The principle of 'privacy by design' should not be made compulsory. It is simply a toolkit which an organisation may use in order to make a risk assessment as to whether a change to existing processes may have data protection compliance issues particularly in connection with the fair and lawful processing principle. FEDMA fully supports the privacy by design initiatives However, it is a concept which is better suited to being introduced via a non – legislative route, such as through codes of practice or self- regulatory initiatives.

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

17. The **right of access** should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the **logic** of the processing?

After a certain point, it is no longer relevant for citizens to gain further access to data system. Behind the privacy area relevant for citizens starts the area of business secrets and companies intellectual property. The logics of processing as a basic business asset should not be covered by right of access. This division between data open to citizens and business data belonging to internal property of company do not prevent citizens from utilizing their right of access at a sufficient level. Moreover, to protect the Privacy of the data subjects, regulatory bodies such as the Data Protection Authorities already have such access to the logic of the processing. They also know how to interpret the logistics.

18. The **right of opposition** is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

Please see our comments above with regard to question 8 on consent which explain the other legitimate grounds for processing apart from consent. The right of opposition where the data processing is not based on the data subject's consent could impose a large economic burden on business.

There is no need to strengthen the "right to oblivion". There is the principle in the Convention that personal information should not be kept for longer than is necessary. More practical guidance on the application of this principle in practice would be welcomed.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

We stress that the Convention should remain principle bases and therefore technology neutral. Special provisions concerning RFID tracking technology belong in the E/Privacy Directive.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

This is impossible. Think of e-commerce (online shopping) and the use of communication means such as e-mail, twitter etc. Besides, the offline world knows no right to remain anonymous in these areas. We do not see any reason why there should be a distinction between the online and the offline world (e.g. a public library's administrative staff knows the users of the library and can observe their reading preferences as well. To satisfy the

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

needs and wishes of its users it will procure more media of any area of interest in which demand is higher. The users of the library thus strongly influence the media offered.) Moreover, this would create problems for law enforcement agencies when dealing with criminal activities.

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

FEDMA does not see the need for introducing class actions for breaches of the Convention. Data protection is inextricably linked to the rights of an individual. It is difficult to see in a class action how individual data subjects could be said to have suffered the same amount of damage or distress, as this will inevitably vary depending on their individual circumstances.

FEDMA would strongly support more scope being given to alternative dispute resolution mechanisms. They are highly effective way of resolving disputes quickly and cheaply.

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

In general, provisions on applicable law must foster one of the core principles of the data protection framework of the signatory, the principle of free movement of personal data. The current Convention 108 ensures a high level of protection of personal data, irrespective of where in the reach of the signatory data are physically stored or where the data controller (or data processor) is established. We are convinced that the current rules on applicable law are effective.
However, we strongly support any practical simplification for companies that engage in European or international cross-border activities. We support a country-of-origin principle, whereby the law of the Member State where the controller is established is applicable. A change in this principle would create significant (and unnecessary) compliance costs for direct marketers who own and operate (cross border/international) databases. Changing the principle from country of origin to country of destination would make it literally impossible to comply with laws in every country around the world where the material would be seen on the Internet. Moreover, it would imply that data controllers treat data relating to data subjects from different Member States differently.

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

We support any practical simplification for companies that engage in European or international cross-border activities but it is perhaps best left up to individual states to consider as it is very complicated and would go against the current emphasis of the Convention on high-level principles.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

Yes. The related fundamental rights were established to protect the individual and his or her liberties from governmental institutions. The private sector can be regulated by consumer protection laws and legislation of other legal areas. However, it would be inadequate to "forget" about the origin of the fundamental rights and their crucial role in the development of the European civil society and democracy. There is no justification for treating the public and private sector generally in an undifferentiated manner. Data protection is first of all a protection of the private individual from the state and an access right against the state. Corporate rules should only be binding in the context of self-regulatory codes. This is no area where the member States should interfere.

Federation of European Direct and Interactive Marketing
5 avenue Ariane, 1200 Brussels, Belgium
Tel: +32 2 779 42 68 - 778 99 20; Fax: +32 2 779 42 69 - 778 99 24
E-mail: info@fedma.org; Web site: http://www.fedma.org

Gesellschaft für Datenschutz
und Datensicherung e. V.

German Association for Data Protection
and Data Security

CONTRIBUTION TO THE QUESTIONNAIRE

FOR STAKEHOLDERS CONSULTATION

01/07/2010

Question 1: **Should the principle of "data minimisation" be explicitly introduced in the legal framework?**

Potentials for data minimization should be used by encouraging data controllers to use pseudonymous data instead of data that are directly related to a person. It should be considered to grant certain benefits to organizations using pseudonymous data and to include a definition of pseudonymous data in the European Directive.

In addition, Article 17 of the Directive could be amended; the new German Federal Data Protection Act (BDSG) explicitly mentions the use of modern encryption procedures as a possible measure to protect personal data. This is not only relevant with regard to the internet but also in the offline world, for example, personal data on portable devices such as notebooks or flash drives should be encrypted.

Question 7: **Is there a need to strengthen the control of a data subject's own personal data? Could the current data protection legislation be improved by establishing a 'property right' over individuals' personal data ("data ownership")?**

Online access, customer and employee self-service could be promoted in order to strengthen the control of a data subject's own personal data.

As far as “data ownership” is concerned, it should be taken into account that according to national legislation companies have to store personal data for certain periods of time for business or tax purposes.

Question 9: Should the current requirement for "unambiguous consent" of the data subject be changed to always require "explicit consent"? If so, how could a requirement for "explicit consent" be implemented and exercised in practice, particularly in the online environment?

"Unambiguous consent" provides the necessary flexibility. The new approach of the German Federal Data Protection Act could be considered; with regard to the protection of customer data Section 28 (3a) BDSG stipulates the following:

.

If consent under Section 4a (1) third sentence is given in a form other than writing, the controller shall provide the data subject with written confirmation of the substance of the consent unless consent was given in electronic form and the controller ensures that the declaration of consent is recorded and the data subject can access and revoke it at any time with future effect. If consent is to be given together with other written declarations, it shall be made distinguishable in its printing and format.

Question 10: Is there a need to improve the modalities of individuals' right of access to their own data, particularly in the online environment?

Secure and cost effective online access procedures can be an appropriate way to guarantee access to the data subject. Therefore, it could be considered to explicitly mention online access and e-mail as possible ways to inform the data subject.

Question 12: Should precise deadlines be introduced for the controller to:

- comply with access requests by data subjects?

- comply with the obligation to rectify or delete data processed in breach of data protection?

It should be taken into account that the time necessary to adequately handle an access or deletion request may vary. This is partially due to the complexity of the IT systems.

Question 13: Should specific safeguards be introduced for the protection of personal data of data subjects with a professional or special official secrecy obligation (e.g. legal profession, medical profession)? If yes, which ones?

No. This can be left to the member states and their national legislation.

Question 14: Is there a need for introducing an explicit principle of transparency into the legal framework in order to ensure that data subjects receive adequate and sufficient information about the collection and processing of their personal data and to enable them to make an informed choice? In particular:

a. Should the information to the data subject contain further compulsory elements,

such as the competent data protection supervisory authority and its contact details?

b. Should the obligation to efficiently display a "privacy notice" which is conspicuous, clear and intelligible to the average user be introduced?

c. Should a uniform EU-format be introduced to comply with this obligation?

Working Paper 100 of the Article 29 Working Party on multi-layered notices already provides valuable guidance that allows for the necessary flexibility.

Question 18: **Should there be specific rules for the processing of personal data in the employment sector?**

a. What issues should be further specified?

b. Would the explicit consent of the data subject be a sufficient and appropriate ground for lawful processing in the employment sector, given the unbalance between the worker and the employer?

c. Is it necessary/opportune to clarify further the conditions/safeguards for processing specific workers' data 'e.g., biometric data, drug and alcohol testing data, Internet/email and other monitoring data?

Some specific rules on the processing of employee data would probably lead to a better harmonization within the EU and also to greater legal certainty for both, employers and employees.

The German Federal Ministry of the Interior is currently preparing a draft for a specific amendment to the Federal Data Protection Act (BDSG). The draft includes provisions on recruitment procedures, health data, fraud and compliance, video surveillance, global positioning systems (GPS), biometric data, e-mail and internet in the workplace and on consent.

Explicit consent of the data subject should remain a possible basis for a lawful processing of employee data. Because of the lack of other legal grounds, there are cases where the employer actually depends on the employee`s consent. The Article 29 Working Party has acknowledged that there are cases where it is appropriate for an employer to rely upon consent, for example, in an international organization where employees wish to take advantage of opportunities in a third country (WP 114, p. 11).

Question 24: **Is there a need to develop alternative dispute resolutions (ADRs) and out-of court proceedings in data protection matters?**

No. The DPAs can take care of dispute resolution. In addition to the DPA, also the internal Data Protection Officer (DPO) may be in charge.

Question 28: Is there a need for further harmonisation of the data protection rules at EU level? Are there practical problems affecting the free movement of data?

Yes. A future legal framework should include a specific provision on the processing of personal data within – multinational – business groups consisting of various legal entities. Especially globalization and new types of outsourcing have created a pressing need for a more flexible processing of personal data within business groups. At the same time a high level of data protection can be maintained by a clear definition of the – shared – responsibilities within such business groups.

In this context the GDD would like to refer to its response to the European Commission Consultation for the Fundamental Right to the Protection of Personal Data.

Question 29: Is there a need to further harmonise, reduce and/or simplify the notification procedures to the DPAs and to ensure an effective follow-up of notifications by the national data protection authorities?

From a GDD point of view notification to the DPA is a rather formal obligation which does not improve the protection of personal data very much. The DPA basically only stores the data until a breach occurs. On the other hand it makes data protection more effective, when notification is done to the DPO who is an internal or external expert familiar with the company`s inner structures and workflows, thus in a position that allows him to actually take care of the data and to be a knowledgeable contact person for the data subject.

Question 30: Should the current provisions on prior checking be revised? If so, how?

Yes. Several so called data protection scandals in Germany have shown an insufficient involvement of DPOs in processing operations. Therefore, it should be clarified that prior information of the DPO about all processing operations involving personal data and – where necessary – prior checking are legally binding requirements. Breaches should be punishable in the Member States.

In this context the GDD would like to refer to its response to the European Commission Consultation for the Fundamental Right to the Protection of Personal Data.

Question 34: Should there be an obligation for controllers to have a DPO? If yes, what would be the threshold for such obligation?

Germany has made good experiences with the DPO for over 30 years *(see Christoph Klug, Improving self-regulation through - law based - Corporate Data Protection Officers; available at http://www.gdd.de/international/english)*. In the past years DPOs have become increasingly accepted by the Member States and by companies around the world. Given the DPOs growing importance, a future Directive should describe the role of the DPO in more detail, including provisions on his appointment, his independent status, his qualifications (initial and continuing training) and his tasks.

Also with regard to harmonization, the function of DPO should be reflected in the laws of each Member State. So far the Directive makes it only optional for Member States to refer to this function into their national laws, which is detrimental to the development of the function . This view is also shared by the French organization AFCDP (Association Française des Correspondants à la Protection des Données). In France, since the Data Protection Act has made this function optional to data controllers, the number of DPOs but also of other data protection professionals has grown, to the benefit of the protection of personal data in the country and of the spreading of a culture of privacy. Like the GDD, the AFCDP believes that in Members States who make the appointment optional, it is important that data controllers appointing DPOs benefit from real incentives (for an example see response to question 29), as appointing a DPO will ensure a more effective data protection.

Question 38: Should the obligation for reporting personal data breach notifications – as currently provided for by the e-Privacy Directive - be extended?

If considering to extend the obligation of security breach notification also to companies not covered by the E-Privacy-Directive (2002/58/EG), a two step approach should be maintained. Generally, information of the data subjects should only be necessary, when the data protection authority has confirmed such a necessity. The obligation should apply to both public and non-public bodies.

From a GDD and AFCDP (Association Française des Correspondants à la Protection des Données) point of view, a sufficient involvement of the DPO should be ensured. The DPO should belong to the prevention and "emergency" team.

In general, any rule within the Directive imposing upon the data controller to notify the authority and /or the concerned individuals should contemplate giving a central and recognized role to the DPO in the process.

Question 46: Should EU data protection legislation apply for any processing of personal data of a data subject residing within the EU, notably when the controller is established outside the EU/EEA?

That could possibly interfere with the sovereignty of other countries.

Question 48: Is the current system of Binding Corporate Rules satisfactory? If not, how can it be improved? Should it be codified in the legal framework?

As the GDD has already pointed out in its response to the European Commission Consultation for the Fundamental Right to the Protection of Personal Data, the BCR procedure needs to be less bureaucratic in order to convince more companies to use BCRs. Mutual recognition by the DPAs is certainly one important aspect in this context.

The German Federal Data Protection Act since 2001 explicitly mentions BCRs as possible adequate safeguards. Article 26 (2) of the European Directive could be amended appropriately in order to emphasize the value of BCRs.

Bonn, July 15th 2010

Gesellschaft für Datenschutz und Datensicherung e. V.

German Association for Data Protection and Data Security

Executive Summary

OF RESPONSE TO EUROPEAN COMMISSION CONSULTATION ON THE LEGAL FRAMEWORK FOR THE FUNDAMENTAL RIGHT TO PROTECTION OF PERSONAL DATA

I. Introduction

The German Association for Data Protection and Data Security (GDD) was founded in 1977 and stands as a non-profit organization for practicable and effective data protection. With more than 2100 – mostly company – members the GDD is Germany`s leading privacy association. Besides offering various member services such as education, training and certification of data protection officers, guides for practitioners and networking opportunities, the GDD also represents member positions at a national and European level, especially as far as new privacy legislation is concerned.

Basically, the GDD shares the view of the European Commission that the Data Protection Directive (95/46/EG) constitutes a general legal framework which fulfils its original objectives by constituting a sufficient guarantee for the functioning of the Internal Market while ensuring a high level of protection (COM(2007) 87 final).

However, the GDD takes the opportunity to participate in this consultation, in order to share some experiences that are based on so-called data protection scandals, changed structures of the data processing within companies and potentials for data minimization and privacy by design.

II. Key Statements

- The role of the ***data protection official*** should be strengthened at the European level. Data protection officials are becoming increasingly accepted by the member states and by companies around the world. However, several so-called data protection scandals have shown an insufficient involvement of data protection officials in processing operations. Therefore, it should be clarified that prior information of the DPO about all processing operations involving personal data and – where necessary – prior checking are legally binding requirements. Breaches should be punishable in the Member States.

- In the future the Data Protection Directive (95/46/EG) should include a specific provision on the processing of personal data within – multinational – ***business groups*** consisting of various legal entities. Especially globalization and new types of outsourcing have created a pressing need for a more flexible processing of personal data within business groups. At the same time a high level of data protection can be maintained by a clear definition of the – shared – responsibilities within such business groups.

- Given the grown importance of ***outsourcing*** in a globalized world and taking into account that Art. 17 of the Data Protection Directive demands for a careful selection of processors and for appropriate controls regarding technical security measures and organizational measures implemented by processors, the Commission should actively support the development of – sector-related – standards that simplify selection and control procedures.

- If considering to extend the obligation of ***security breach notification*** also to companies not covered by the E-Privacy-Directive (2002/58/EG), a two step approach should be maintained. Generally, information of the data subjects should only be necessary, when the data protection authority has confirmed such a necessity. The obligation should apply to both public and non-public bodies.

- ***Potentials for data minimization*** should be used by encouraging data controllers to use pseudonymous data instead of data that are directly related to a person. It should be considered to grant certain benefits to organizations using pseudonymous data and to include a definition of pseudonymous data in the European Directive.

Bonn, December 17th 2009

Stellungnahme

der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD)

im Rahmen der Konsultation der Europäischen Kommission zum Rechtsrahmen für das Grundrecht auf Schutz personenbezogener Daten

I. Vorbemerkung

Die GDD tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie verfolgt das Ziel, die Daten verarbeitenden Stellen – insbesondere auch deren Datenschutzbeauftragte – bei der Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen. Die GDD wird getragen von mehr als 2.100 Unternehmen, Behörden und persönlichen Mitgliedern. Sie stellt damit die größte Vereinigung ihrer Art und zugleich einen der größten Verbände in der Informations- und Kommunikationsbranche in Deutschland dar.

Im Wesentlichen teilt die GDD die Auffassung der Kommission (COM(2007) 87 final), dass die Grundsätze der Richtlinie 95/46/EG nach wie vor tragfähig sind. Sie nimmt die aktuelle Konsultation der Kommission aber zum Anlass, auf einige Erfahrungswerte hinzuweisen, die insbesondere auf festgestellten Missständen, geänderten Strukturen der Datenverarbeitung in der Wirtschaft bzw. in Konzernen sowie auf Verbesserungspotenzialen im Bereich der Datensparsamkeit und der datenschutzfreundlichen Technikgestaltung basieren. Dabei fokussiert sich die GDD im Rahmen der nachstehenden Ausführungen primär auf die Vorgaben der allgemeinen Datenschutzrichtlinie (95/46/EG).

II. Stärkung der Rechtsstellung betrieblicher Datenschutzbeauftragter auf EU-Ebene

Aus gegebenem Anlass bedarf es aus Sicht der GDD einer Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten.

Die ursprünglich von der GDD mit angeregte Aufnahme des betrieblichen Datenschutzbeauftragten in die EU-Datenschutzrichtlinie (95/46/EG) hat zu einer gewissen Internationalisierung der betrieblichen Selbstkontrolle im Datenschutz geführt (vgl. Klug, RDV 2005, 163). Ersichtlich haben neben Deutschland auch Estland, Frankreich, Luxemburg, Malta, die Niederlande, Schweden und die Slowakei den Datenschutzbeauftragten in ihren Datenschutzgesetzen verankert. So wie es auch in der Richtlinie 95/46/EG angelegt ist, ist die Bestellung von Datenschutzbeauftragten in den meisten Ländern optional. Auch in den USA, wo keine diesbezüglichen gesetzlichen Regelungen bestehen, werden vielfach sog. Corporate Privacy Officers eingesetzt, was den Mehrwert der betrieblichen Selbstkontrolle im Datenschutz untermauert.

Inzwischen hat sowohl die EU-Kommission (COM(2003) 265 final – Report, S. 18 und 24) als auch die Datenschutzgruppe nach Art. 29 der EU-Datenschutzrichtlinie (WP 106, S. 22 und 23) die Bestellung betrieblicher Datenschutzbeauftragter – nicht zuletzt unter dem Blickwinkel der Entbürokratisierung – offiziell empfohlen. Die Artikel 29-Gruppe hat mit Blick auf eine mögliche allgemeine Etablierung des Datenschutzbeauftragten im WP 106, S. 24 folgende Aussage getroffen:

„Bei der Erwägung der Möglichkeit, Datenschutzbeauftragte allgemein zu etablieren, d. h. von administrativer zu interner Aufsicht überzugehen, sind sowohl die bisher in den Mitgliedstaaten mit der Anwendung der Rechtsvorschriften gesammelten Erfahrungen als auch die dortigen Rechtskulturen entsprechend zu berücksichtigen."

Dem ist uneingeschränkt zuzustimmen. Aber auch wenn die Bestellung von Datenschutzbeauftragten nach der EU-Datenschutzrichtlinie optional ist, so knüpft die Richtlinie an den Umstand der Bestellung doch gewisse Privilegierungen, speziell hinsichtlich der ansonsten bestehenden Meldepflicht. Allerdings setzt die Richtlinie in diesem Zusammenhang gleichzeitig eine effektive Datenschutzkontrolle bzw. ihrem Wortlaut nach die „Sicherstellung" der Umsetzung der nationalen Datenschutzvorschriften durch den Datenschutzbeauftragten voraus. Diese Voraussetzungen sind natürlich nicht erfüllt, wenn die Datenschutzbeauftragten über wichtige Datenverarbeitungsprozesse erst gar nicht informiert werden.

Vor diesem Hintergrund bedarf es aus Sicht der GDD einer Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten. Wie der Vorstandsvorsitzende der GDD, Prof. Peter Gola anlässlich der Datenschutzkonferenz der EU-Kommission im Mai 2009 in Brüssel bereits aufzeigen konnte, waren viele der zuletzt bekannt gewordenen „Datenschutzskandale" dadurch gekennzeichnet, dass die betrieblichen Datenschutzbeauftragten über die geplante Datenverarbeitung nicht oder nicht rechtzeitig informiert waren. Infolgedessen konnten Sie auch nicht, wie von der EU-Datenschutzrichtlinie vorausgesetzt, auf die Einhaltung der Datenschutzvorschriften hinwirken. Um derartigen Umgehungen des Datenschutzbeauftragten in Zukunft vorzubeugen, bietet es sich an, seine unabhängige Kontrollfunktion – ggf. durch eine

explizite Regelung in der EU-Datenschutzrichtlinie – dahingehend zu konkretisieren, dass der Datenschutzbeauftragte im Rahmen der Einführung von Verfahren automatisierter Datenverarbeitung zwingend rechtzeitig zu beteiligen ist. Für den Fall einer Zuwiderhandlung sollten in den nationalen Datenschutzgesetzen Rechtsfolgen vorgesehen werden. Dies gilt insbesondere auch im Hinblick auf die von den Datenschutzbeauftragten nach der EU-Datenschutzrichtlinie vorzunehmende Vorabkontrolle.

Auch im Rahmen der anlässlich der 31. Internationalen Datenschutzkonferenz verabschiedeten „Madrid-Resolution“ ist auf die zentrale Bedeutung vorbeugender Datenschutzmaßnahmen hingewiesen worden. Hierzu wird ausdrücklich auch die Bestellung von qualifizierten und mit den notwendigen Mitteln und Befugnissen ausgestatteten betrieblichen Datenschutzbeauftragten gezählt.

Gemäß Art. 8 Abs. 3 der EU-Grundrechte-Charta muss die Einhaltung der Datenschutzgrundrechte von einer unabhängigen Stelle überwacht werden. Auch dies bedingt im Fall der internen Datenschutzkontrolle durch betriebliche Datenschutzbeauftragte deren rechtzeitige Einbindung in die Datenverarbeitungsprozesse.

III. Einführung einer Konzernregelung

1. Ausgangslage

Die GDD befürwortet die Aufnahme einer Konzernregelung in die EU-Datenschutzrichtlinie.

Gerade in den letzten Jahren ist das Anliegen der Schaffung einer Konzernregelung verstärkt aus dem Kreis ihrer Mitglieder an die GDD herangetragen worden. Zunehmend werden unternehmerische Ziele in nationalen und multinationalen Unternehmensverbünden verfolgt, wobei die Konzerne im wachsenden Maße darauf angewiesen sind, Kunden- und Mitarbeiterdaten im Rahmen ihrer Geschäftstätigkeiten an konzernangehörige Unternehmen zu transferieren. Hinzu kommt, dass die Konzernstrukturen einer großen Dynamik unterworfen sind und konzerninterne Dienstleistungen häufig zentralisiert oder arbeitsteilig erbracht werden (z. B. bei Shared-Service-Centern bzw. bei Matrixstrukturen in der Vorgesetztenhirarchie). Vor dem Hintergrund dieser Entwicklungen bedarf es nach Auffassung der GDD einer zeitgemäßen Fortentwicklung der Vorschriften hinsichtlich der Datenschutzverantwortlichkeiten im Konzern.

Während Konzerne sich als wirtschaftliche Einheit verstehen und dementsprechend agieren, ist nach der Begründung des geänderten Richtlinienvorschlags der Kommission (vom 15. Oktober 1992, COM (92) 422 endg. - SYN 287 - ABl. Nr. C 311 vom 27.11.1992, 30) datenschutzrechtlich das einzelne Unternehmen als juristische Person maßgeblich. In der Begründung heißt es wörtlich:

„Personen, die in einem anderen Unternehmen arbeiten, auch wenn dieses demselben Konzern oder derselben Holding angehört, dürfen im allgemeinen als Dritte an-

gesehen werden."

Dies steht allerdings in einem gewissen Widerspruch zu der Legaldefinition in Art. 2 Buchstabe d der EU-Datenschutzrichtlinie und lässt die gesellschaftsrechtlichen und wirtschaftlichen Zusammenhänge im Wesentlichen unberücksichtigt. Die Begriffsbestimmung in Artikel 2 Buchstabe d der Richtlinie stellt auf den „für die Verarbeitung Verantwortlichen" ab. Dies ist nach der Legaldefinition die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein „oder gemeinsam mit anderen" über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Diese Entscheidungsgewalt liegt de facto vielfach bei den Konzernmüttern (z.B. auf Grund von Beherrschungsverträgen). Häufig sind Verarbeitungsprozesse aber auch auf verschiedene Konzernteile verteilt, so dass damit einhergehende Entscheidungen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten gemeinsam mit anderen getroffen werden können.

Die Aufnahme einer klarstellenden Regelung, die derartige konzerntypische Verarbeitungsprozesse unter klarer Definition der – geteilten – datenschutzrechtlichen Verantwortlichkeiten abbildet, in die EU-Datenschutzrichtlinie würde sowohl der Rechtsklarheit als auch der betrieblichen Wirklichkeit Rechnung tragen und damit einen zeitgemäßen Beitrag zur Akzeptanz der Richtlinie leisten. Vor diesem Hintergrund und insbesondere mit Blick auf den von der EU-Datenschutzrichtlinie bezweckten freien Datenverkehr innerhalb der EU (vgl. Erwägungsgrund 3 der Richtlinie) erachtet die GDD es als sinnvoll, den gewandelten Gegebenheiten im Rahmen einer Spezialregelung für verbundene Unternehmen unter Wahrung eines angemessenen Datenschutzniveaus Rechnung zu tragen.

2. Umsetzungsprobleme im Konzern

a) Abgrenzung Auftragsdatenverarbeitung / Datenübermittlung an Dritte

Mit Blick auf die Zulässigkeit der Datenverarbeitung bedarf es im Konzernverbund vielfach der Abgrenzung zwischen einer Datenverarbeitung im Auftrag nach Art. 17 der EU-Datenschutzrichtlinie und einer Datenübermittlung an Dritte. Angesichts der Vielfältigkeit neuartiger Outsourcingkonstellationen fällt diese Beurteilung in der Praxis oft schwer. Dies ist auch darauf zurückzuführen, dass Konstruktionen zugenommen haben, bei denen Auslagerungen nicht nur eine Unterstützungshandlung bei der Datenverarbeitung beinhalten, sondern auch mit der Übertragung inhaltlicher Aufgaben einher gehen (vgl. GDD-Arbeitskreis „Datenschutzpraxis", Praxishilfe V, S. 8 f. sowie Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datenverkehr", abrufbar unter www.rp-darmstadt.hessen.de).

Mit der Schaffung einer Konzernregelung könnten diese Abgrenzungsschwierigkeiten beseitigt und durch klare Verantwortlichkeitsregelungen ersetzt werden.

b) Datenschutzrechtliches Vertragsmanagement

Nicht zuletzt die Zentralisierung von Datenverarbeitungsprozessen im Konzern führt dazu, dass zahlreiche Konzernabteilungen die Funktion eines internen Dienstleisters im Konzern übernehmen. Dementsprechend fungieren die Konzerngesellschaften

untereinander als Dienstleister. Vor diesem Hintergrund und mit Blick auf die große Dynamik, der Konzernstrukturen unterworfen sind, sollte ein allzu bürokratisches Vertragsmanagement vermieden werden.

Art. 17 der EU-Datenschutzrichtlinie fordert detaillierte und individuelle schriftliche Festlegungen, die im Rahmen konzerninterner Dienstleistungen zu einer unüberschaubaren Vielzahl von – ggf. alsbald wieder anzupassenden – vertraglichen Regelungen führen können. Organisatorische Änderungen im Bereich des Einsatzes konzerninterner Dienstleister (z. B. die Zentralisierung von Rechenzentren bzw. die Verselbständigung von Unternehmensbereichen) müssten jeweils durch neue oder angepasste Datenschutzvereinbarungen flankiert werden, selbst wenn sich die Aufgaben und Zugriffsrechte der Personen durch die Umorganisation nicht verändern. Insofern sollten Rahmenvereinbarungen (ggf. unter Einbeziehung konzernweit geltender Datenschutz- und Datensicherheitsregelungen) möglich bleiben, um den Konzernen einen übermäßigen administrativen Aufwand zu ersparen und ihnen die nötige Flexibilität zu gewährleisten.

Art. 17 der Richtlinie verpflichtet die Auftraggeber ferner zu einer sorgfältigen Auswahl und Kontrolle hinsichtlich der vom Auftragnehmer zu treffenden technischen und organisatorischen Sicherheitsmaßnahmen. Zahlreiche GDD-Mitglieder haben darauf hingewiesen, dass die Etablierung gewisser Standards eine ordnungsgemäße Auswahl- und Kontrolle von Auftragnehmern erheblich vereinfachen würde. Vor diesem Hintergrund und angesichts der gewachsenen Bedeutung der Auftragsdatenverarbeitung sollte die Entwicklung von – branchenspezifischen – Marktstandards im Sinne von Best Practices bzgl. der Auswahl bzw. der Kontrolle von Datenverarbeitungsdienstleistern von der EU-Kommission aktiv gefördert werden.

c) Mitarbeiterdaten im Unternehmensverbund

Im sog. konzerndimensionalen Arbeitsverhältnis besteht für die entsprechenden Mitarbeiter in der Regel eine hinreichende Transparenz hinsichtlich der konzernweiten Verwendung ihrer Daten. Nicht immer aber stellt sich ein Konzern aus Sicht der Beschäftigten als homogene Einheit dar. Auf Grund des Fehlens einer Konzernregelung in der EU-Datenschutzrichtlinie besteht auch hinsichtlich der datenschutzgerechten Verwendung von Mitarbeiterdaten im Unternehmensverbund erhebliche Rechtsunsicherheit. Der Einsatz eines Shared-Service-Centers „Human Ressources“, die Datenweitergabe an Matrix-Vorgesetzte, zentralisierte E-Mail- oder Internet-Server, die Pflege eines konzernweiten Skill-Managements, konzernweite elektronische Kommunikationsverzeichnisse, Whistleblowing und Bonusprogramme wie Aktienoptionspläne seien insofern hier nur beispielhaft genannt.

Im Rahmen einer Konzernregelung sollte in Ergänzung zu Art. 8 Buchstabe b der EU-Datenschutzrichtlinie klargestellt werden, dass auch wirtschaftliche Interessen bzw. Interessen an einer Optimierung der Geschäftstätigkeit in Konzernen die Übermittlung von Mitarbeiterdaten rechtfertigen können, soweit berechtigte Interessen der Mitarbeiter nicht entgegenstehen.

d) Grenzüberschreitende Datenflüsse im Konzern

Zunächst ist nochmals darauf hinzuweisen, dass die EU-Datenschutzrichtlinie auch einen freien Datenverkehr im europäischen Binnenmarkt bezweckt und insofern unnötige Hindernisse schon unter Harmonisierungsgesichtspunkten zu vermeiden sind.

Aber auch mit Blick auf den Datentransfer an in Drittländern ansässige Konzernunternehmen sollten im Rahmen der Schaffung einer Konzernregelung vorhandene Rechtsunsicherheiten beseitigt werden. So sollte beispielsweise klargestellt werden, dass die Datenweitergabe an in Drittländern ansässige Unternehmen, die ein angemessenes Datenschutzniveau aufweisen, nicht als Datenübermittlung an Dritte anzusehen ist. Wenn die Privilegierung der Auftragsdatenverarbeitung innerhalb der EU bzw. des EWR greift, weil auf Grund der Harmonisierung durch die EU-Datenschutzrichtlinie insofern vom Vorliegen eines angemessenen Datenschutzniveaus auszugehen ist, so sollte Entsprechendes aus Gründen der Gleichbehandlung auch für Unternehmen im Drittland gelten, soweit diese ihrerseits ein angemessenes Datenschutzniveau hergestellt haben (vgl. Müthlein/Heck, Outsourcing und Datenschutz, 3. Aufl. 2006, S. 73 f.; Klug, RDV 2000, 212, 2215). Aus Gründen der Harmonisierung bzw. der Rechtseinheitlichkeit innerhalb der EU sollte auch die insofern bestehende Folgeverpflichtung der Mitgliedstaaten betont werden. Gleiches gilt hinsichtlich der Akzeptanz von EU-Standardverträgen durch die nationalen Datenschutzaufsichtsbehörden.

Ferner sollte zeitnah ein koordiniertes – möglichst unbürokratisches – Genehmigungsverfahrens bei der Verwendung von Binding Corporate Rules (BCRs) etabliert werden, da ansonsten die Gefahr besteht, dass die Unternehmen von dieser Möglichkeit der Gewährleistung angemessener Datenschutzgarantien nicht in dem gewünschten Umfang Gebrauch machen. Gegebenenfalls sollte die Garantiefunktion von BCRs ausdrücklich in Art. 26 Abs. 2 der Richtlinie erwähnt werden.

Aus gutem Grund ist in der „Madrid-Resolution“ insgesamt auf die Notwendigkeit einer Vereinheitlichung des Datenschutzes durch eine verstärkte Kooperation und Koordinierung der Datenschutzaufsichtsbehörden sowohl auf internationaler als auch auf nationaler Ebene hingewiesen worden.

IV. Informationspflicht bei Datenverlusten / Security Breach Notification

Soweit auf EU-Ebene erwogen werden sollte, die für Provider nach der E-Privacy-Richtlinie (2002/58/EG) bereits geltende Informationspflicht bei bestimmten Datenverlusten auch auf andere Unternehmen zu erstrecken, so ist zunächst darauf hinzuweisen, dass dies in Deutschland mit der Einfügung von § 42a BDSG bereits erfolgt ist. Allerdings sieht die deutsche Regelung vom Grundsatz her eine unverzügliche Information sowohl der Datenschutzaufsichtsbehörde als auch der Betroffenen vor.

Unter dem Aspekt der Verhältnismäßigkeit ist im Rahmen einer Benachrichtigungspflicht bei Datenverlusten aber ein zweistufiges Verfahren anzuraten, wie es im Übrigen auch in der Datenschutzrichtlinie für die elektronische Kommunikation angelegt

ist. Danach ist primär die Aufsichtsbehörde zu benachrichtigen. Wird der zuständigen Datenschutzbehörde nachgewiesen, dass die verantwortliche Stelle bereits geeignete Schutzmaßnahmen für die Daten der Betroffenen ergriffen hat, ist eine Information der Betroffenen entbehrlich bzw. gegebenenfalls unter dem Gesichtspunkt der unnötigen Beunruhigung der Betroffenen sogar kontraproduktiv.

Ferner sollten die Informationspflichten gleichermaßen für nicht-öffentliche und öffentliche Stellen gelten, da für eine unterschiedliche Behandlung dieser Bereiche kein sachlicher Grund erkennbar ist.

V. Datenschutz durch Technik / Privacy by Design

Angestrebt werden sollte eine gewisse Privilegierung pseudonymer Datenverarbeitung, um die Anwendung des Grundsatzes der Datenvermeidung und Datensparsamkeit zu fördern bzw. um das Mitführen der Identität der Betroffenen im Rahmen von Datenverarbeitungsprozessen zu reduzieren. Wenn die Verarbeitung pseudonymisierter Daten stets zur vollen Anwendbarkeit sämtlicher Vorschriften der EU-Datenschutzrichtlinie führt, mangelt es den Unternehmen gegebenenfalls an der nötigen Motivation, die Daten zunächst ohne unmittelbaren Personenbezug und damit auf datenschutzfreundliche Art und Weise zu verarbeiten. Hier könnten neue Anreize gesetzt werden.

Die rechtzeitige Berücksichtigung des Datenschutzes schon bei der Entwicklung von IT-Systemen sollte nachhaltig gefördert werden.

VI. Beibehaltung technologieneutraler Regelungen

Im Hinblick auf die Zukunftsfähigkeit der EU-Datenschutzregelungen sollte auch weiterhin auf technologieneutrale Regelungen gesetzt werden.

Bonn, den 17. Dezember 2009

Gesellschaft für Datenschutz
und Datensicherheit e. V.

German Association for Data Protection
and Data Security

CONTRIBUTION TO

CONSULTATION ON THE COMMISSION´S

COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION

IN THE EUROPEAN UNION

COM(2010) 609 final

I. INTRODUCTION

The German Association for Data Protection and Data Security (GDD) was founded in 1977 and stands as a non-profit organization for practicable and effective data protection. With more than 2200 – mostly company – members the GDD is Germany`s leading privacy association. Besides offering various member services such as education, training and certification of Data Protection Officers, guides for practitioners and networking opportunities for data protection professionals all across Germany, the GDD also represents member positions at a national and European level, especially as far as new privacy legislation is concerned.

In addition to the contributions already made (Stakeholders' Conference 2009, Public Consultation 2009, Stakeholders' Consultation 2010), the GDD welcomes the opportunity to make some additional remarks on the Communication from the Commission - COM(2010) 609 final.

II. REDUCING THE ADMINISTRATIVE BURDEN

The GDD welcomes the Commission`s intention to reduce administrative burdens, especially with regard to the current notification system. At the same time, the GDD shares the Commission`s view according to which administrative simplification should not lead to an overall reduction of the data controllers' responsibility in ensuring effective data protection.

In previous contributions the GDD already pointed out the necessity to improve internal control mechanisms and welcomes the Commission`s intention to spell out appropriate obligations in more detail.

From a GDD point of view, the reduction of administrative burdens can be balanced by strengthening the role of the Data Protection Officer. Appointing a Data Protection Officer is not an additional burden for controllers. Companies in Member States have to comply with data protection law anyway and "somebody has to do the job".

III. STRENGTHENING THE ROLE OF THE DATA PROTECTION OFFICER (DPO)

1. Perspective of the Commission

According to Communication COM(2010) 609 final, the Commission will consider to enhance data controllers' responsibility by

- *making the appointment of an independent Data Protection Officer mandatory, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;*

- *harmonising the rules related to the Data Protection Officer`s tasks and competences.*

2. Mandatory Data Protection Officer

a) Growing acceptance of the DPO around the world

As expressed in previous GDD contributions, Germany has made good experiences with the Data Protection Officer within the past 30 years and DPOs are becoming increasingly accepted by Member States and by companies around the world.

On the occasion of the 31st International Conference on Data Protection and Privacy data protection authorities from over 50 countries approved the "Madrid Resolution" on international privacy standards. One of the most relevant chapters of the document is the one that refers to proactive measures. It includes the recommendation to appointment Data Protection or Privacy Officers, with adequate qualifications, resources and powers for exercising their supervisory functions adequately.

b) Appropriate threshold

Making the DPO mandatory at EU level could help to achieve the goal of improving internal control mechanisms. The GDD agrees with the Commission on the necessity of avoiding undue administrative burdens, particularly on small and micro-enterprises. However, the ***number of persons employed*** for the purpose of processing personal data is only one of several

factors that should be taken into account. After all, the risks to the rights and freedoms of the data subjects depend on the circumstances of the individual case.

With regard to a possible obligation to appoint a Data Protection Officer, the GDD suggests to also take into account the following criteria:

- ***Amount of personal data being processed***

Companies processing large amounts of personal data are more likely to put the rights and freedoms of the data subjects at risk than companies only dealing with a minimum of personal data. Generally, companies where the processing of personal data is a major part of the overall business purpose (e.g. internet or telecommunication service providers) have a higher risk potential, because of the large amounts of personal data being processed.

The same applies to companies processing personal data on behalf of their clients. The GDD agrees with the Commission that internal control mechanisms are especially important *"in those increasingly common cases where data controllers delegate data processing to other entities (e.g. processors)."* Even if the controller remains responsible in such cases, it is essential to have a knowledgeable contact person within the processor.

- ***Purpose of processing operations***

A higher risk potential could also be attributed to companies which commercially carry out automated processing of personal data for the purpose of transferring them to other parties (e. g. companies trading mailing lists). The same applies to organizations processing personal data for market or opinion research purposes.

Generally, the profiling of personal data – e.g. by credit agencies – involves specific risks for the rights and freedoms of the data subjects.

- ***Sensitivity of data***

According to the German Federal Data Protection Act (BDSG), the obligation to appoint a DPO applies in all cases where prior checking is required. That may include the processing of sensitive data according to Article 8 (1) of EU Directive (95/46/EC). Health data, for example, are being processed not only by hospitals but also by insurance companies. Also the financial sector highly depends on a confidential handling of personal data (e. g. with regards to bank or credit card information).

c) Alternative: The DPO as an option

In case the Commission decides not in favor of a mandatory DPO, the GDD recommends the following:

Also with regard to harmonization, the function of DPO should be reflected in the laws of each Member State, at least as an option. This view is also shared by the French organization AFCDP (Association Française des Correspondants à la Protection des Données). In France, since the data protection law has made this function optional to data controllers, the number of DPOs but also of other data protection professionals has grown, to the benefit of the protection of personal data and the spreading of a culture of privacy in the country.

Companies making use of the option to appoint a DPO should benefit from real incentives, since the DPO will ensure more effective data protection, thus unburden the DPA.

2. Harmonizing / specifying the role of the DPO

The Directive 95/46/EC is not very specific with regard to the role of DPOs, their appointment, their tasks, their independent status and their qualifications. German law includes much more detailed information on the role of the DPO which may serve the Commission as a source of information (for an overview see article by *Christoph Klug*, Improving self-regulation through - law-based - Corporate Data Protection Officials; available at http://www.gdd.de/international/english).

In addition, the GDD would like to make the following recommendations:

Appointment: In some Member States there is an obligation to register the appointed DPO with the Data Protection Authority (DPA). Some DPAs keep a list of the appointed DPOs which is publicly available. In favor of harmonization and transparency for DPAs and data subjects an EU wide obligation to register the appointed DPO with the competent DPA could be considered.

Tasks and duties: The GDD once again (see previous contributions) emphasizes the necessity to clarify that generally prior information of the DPO about all processing operations involving personal data and – where necessary – prior checking are legally binding requirements.

The recent revision of the e-Privacy Directive introduced a mandatory personal data breach notification covering, however, only the telecommunications sector. This provision was already transposed in German law. The German legislator even went a step further by amending a general provision on breach notification to the Federal Data Protection Act (Section 42a BDSG) which covers the entire private sector. Given the fact that the Commission will examine the modalities for extending the obligation to notify personal data breaches to other sectors, it should be clarified that the DPO should belong to the prevention and emergency team and that the DPO should become involved in the notification procedure.

Complete independence: In order to enable the DPOs to perform their job effectively they have to be guaranteed the necessary powers, means, premises, facilities, equipment and

resources. Once appointed, the DPOs should be in a position to make their own professional judgement. Regarding their independence, it is essential for DPOs to have the right to directly report to the board of directors, respectively to the company management. According to German law the DPO "shall be directly subordinate to the head of the public or private body".

Generally, the role of the DPO should not be reduced to a mere compliance function. With the growing risks for the rights and freedoms of data subjects the DPO`s role should become more influential and more strategic.

Qualifications: Only qualified DPOs may perform their increasingly important job effectively. Therefore, a future directive should include at least some essential job prerequisites.

The GDD conducted a study on the necessary qualifications.

The results of the study have recently been confirmed by German DPAs http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.pdf?

According to the GDD study the DPO should have

- a profound knowledge of data protection law,
- an adequate knowledge of IT standards,
- the ability to establish a proper data protection management, based on an adequate knowledge of business related economics and a specific knowledge of the company`s inner structures and processing operations.

Based on this study, the GDD has developed an educational program for data protection professionals, including a certification program for DPOs (GDDcert).

Since 2009, the German Federal Data Protection Act includes a provision according to which the controller must allow and pay for an adequate education of the DPO.

IV. DATA PROCESSING WITHIN – INTERNATIONAL – BUSINESS GROUPS

The Commission aims to *clarify and simplify the rules for international data transfers*.

In addition to the contributions already made, the GDD would like to mention that the German Government (BT-Drs. 17/4230) shares the view of the Federal Council (Bundesrat - BR-Drs. 535/10) according to which questions arising from the processing of personal data within business groups need further investigation and need to be discussed in connection with the revision of the European Directive (95/46/EC).

Bonn, January 7th 2011

GERMAN INSURANCE ASSOCIATION

Preliminary remark The German Insurance Association (GDV) is the umbrella organisation for private insurers in Germany. Its 469 member companies, with around 228 000 employees and trainees, offer comprehensive coverage and provisions to private households, trade, industry and public institutions, through more than 430 million insurance contracts. As a risk taker and major investor, the insurance industry has outstanding significance in connection with investments, growth and employment in the German economy. The German insurance industry welcomes the initiative taken by the Council of Europe to review its Convention 108. Since for the conclusion and performance of insurance contracts insurance companies rely on personal data and sensitive data, especially health data, new data protection regulations are of high relevance to them. The German insurance industry endorses the objective of the Council of Europe of reviewing Convention 108, focusing on technological developments of the information and communication society and globalisation of data processing operations. In this respect, the identification of regulatory gaps in the area of new technologies, especially the Internet, poses a major challenge. By contrast, from the point of view of the German insurance industry, as far as traditional data processing operations in the so-called offline world are concerned, the current data protection regulations have proven their value. Therefore, in creating **new requirements**, it should be **carefully looked into the question as to whether and to what extent they may also be applied to the offline world** (see under 1. and 18.) For **data flows within insurance groups**, between direct insurance and reinsurance companies and for the shifting of tasks towards service providers, an **adjustment of the definition of the controller of the file** would be appropriate. In the case of centralised data processing within a group, the companies transferring the data and the company assuming the respective task on behalf of the other companies could be considered jointly as controller. If certain safeguards are met, an economically appropriate shifting of tasks to external service providers should be made possible (for details see under 5.). If further specifications for a **declaration of consent** under data protection legislation are considered, first of all, the question arises as to whether or not this legal instrument is appropriate for areas which imperatively require data uses. The voluntariness of the consent is questioned by the German data protection authorities if there is no alternative to the consent (for details see under 8. / 9.). For this reason, the German data protection authorities officially advocate a **rule on the processing of health data by the insurance industry.**

1. Technologically neutral approach

Technologically neutral data protection rules are important to cover future technologies as well, if possible. Nonetheless, technical neutrality cannot mean that rules are adopted for areas where they are not required. Consideration should be given to the higher risk exposure in the case of data processings on the Internet as compared with data processings which can be clearly attributed to a controller. With a view to new technologies, a first step should consist in looking into the question as to whether and to what extent existing data protection requirements may be applied to these. If new rules should actually be required, it should be looked into the question as to whether these should be limited to the new technologies and whether tradititional data processings in the offline world may remain unaffected.

2.-4. . /.

5. Definition of the controller of the file

The German insurance industry would welcome a review of the definition of the controller of the file because this would provide the opportunity to allow for the changes in data processing in business. This concerns above all the centralisation of service tasks within insurance groups just as in other sectors and the outsourcing of tasks to competent service providers, which – using the new technologies – is meanwhile possible, even across borders, and also appropriate to achieve synergies and to meet the requirement of economy. For instance, in insurance groups, risk assessment is frequently carried out centrally by one company of the group, in order to combine know-how and the required technical equipment rather than to have to hold it available for every insurance line. However, problems arise in practice if any data transfer from one company of the group to another company cannot be based on legitimate grounds and if a consent has to be obtained from the customer instead. This would unnecessarily impede the centralization of tasks. In the insurance industry, these problems cannot be solved by simply merging companies. In fact, according to Article 73 of the Directive 2009/138/EC, insurance companies are, as a matter of principle, bound to observe the principle of separation of lines between life and nonlife insurance. These insurance lines may be carried on only by different legal entities. In Germany, the requirements on separation of lines are even stricter. If the Council of Europe now discusses the inclusion of legitimate grounds in Convention 108 (see Question 9), this potential area of conflict should be taken into account. As a possible solution, a simplification for groups might be included in the definition of the controller of the file. For instance, with regard to centralization of tasks in a group, the transferring company and the receiving company might be considered jointly as one controller. For the outsourcing of tasks to service providers a simplification might be provided for if it is ensured that the data are processed only in line with the original purpose, that the other companies have been selected carefully taking into account the appropriateness of the technical and organizational measures taken by them with respect to data protection and data security and if, moreover, it has been agreed in the contract that the other company offers the same guarantees of the protection of confidential information and of data protection as the insurance company itself.

6. Definition of processor / definition of personal data

A definition of processor should be flexible and allow for the circumstance that also the parent company may be mandated by a group company as processor, but that in this case there are limits for granting authority to issue instructions according to existing law. The concept of personal data should be restricted for data that mainly refer to objects to the effect that the data controller (and not any other body) may link the data in the respective context without much effort to a person. There are uncertainties as to whether or not data protection rules are applicable in certain cases. Data protection legislation has to confine itself to cases in which the right to informational self-determination is actually affected. In the case of data on objects, this is frequently difficult to assess. Modern technology has significantly increased the theoretical possibilities to link data with and without personal reference to each other. Data that actually only refer to an object, such as, for instance, the location of a property or features of a motor vehicle, can be linked to a person or often even to several persons who are more or less closely related to this object. For instance, a property which appears in a map or a geo-information system can be linked to its owner, tenant or leaseholder. A motor vehicle can be linked to its present or former owners, registered keepers, drivers and policyholders. Data protection legislation has to interfere if the data on objects are actually linked to a person or if the controller could do this without facing any technical or legal difficulties. However, there is a risk that data on objects are considered as personal data because of the theoretical possibility to link the data, and that the scope of application of data protection legislation would become boundless.

7. New principles – data minimisation principle

According to the current requirement of Art 5 (b), (c) of Convention 108, personal data may only be stored for specified and legitimate purposes. The data must be adequate, relevant and not excessive in relation to these purposes, which already constitutes a restriction. In addition to the implementation of this requirement, German law contains the express principle of data avoidance and data economy for the organization and selection of data processing systems (Sect. 3a of the Federal Data Protection Act [*Bundesdatenschutzgesetz - BDSG]*). In the data collection and data processing operations of the insurance industry these requirements are complied with. However, for the assessment and calculation of an individual risk, insurance companies need comprehensive information, so that the community of insureds is not unnecessarily put at a disadvantage due to bad risks. Subsequently, from the point of view of the legal obligation to produce supporting documents (regulations of commercial and tax law) and for reasons of traceability (revision), the information used has also to be stored for a certain period. our point of view, more restrictive rules are not required. To ensure the necessary flexibility for companies, any principle of data economy should, if possible, not be designed as an obligation, but as a target.

8. / 9. Consent / legitimate processing

a. Inclusion of requirements on consent and legitimate grounds

Unlike Directive 95/46/EC, Convention 108 contains neither legitimate grounds for data uses nor prerequisites for consent. By contrast, Directive 95/46/EC establishes differentiated requirements for consent and the processing of personal data (Article 7) and special categories of personal data (Article 8). If rules on consent and legitimate grounds are included in Convention 108, these should not be worded more restrictively than the requirements stated in Directive 95/46/EC.

Especially with a view to the desirable accession of further states to Convention 108, rules with a high level of abstraction are appropriate. Too narrow legitimate grounds involve the risk that they will lead to conflicts in practice. Sufficent scope of interpretation and ability to design may allow for national as well as sector-specific particularities of both accession candidates and signatory states. Alternatively, exception and opening clauses may be envisaged. The exception from the ban on the processing of sensitive data in the case of consent of the data, provided for in Directive 95/46/EC, causes problems, for instance in the insurance industry. Therefore, any possible inclusion in Convention 108 should be handled carefully. According to the current legal situation, a data subject has to sign a declaration of consent if he wants to conclude an insurance contract for which health data are relevant. It is indispensable to process health data within the scope of insurance contracts, for instance, for establishing and performing contracts in life, health and accident insurance and partly also in third party liability insurance, insurance companies have to collect and process health data.

As according to Art. 2 (h) of Directive 95/46/EC a consent has to be given freely (under German law: based on a free decision), while there is no alternative at all to making a declaration of consent in this case, the prerequisite of voluntariness is doubted by the German data protection authorities. This leads to considerable legal uncertainty for insurance companies. Therefore, the German insurance industry, in agreement with the German data protection authorities, demands the creation of a basis of permission in Art. 8 (2) of Directive 95/46/EC. When health data are processed, according to Directive 95/46/EC, a consent of the data subject is as a matter of principle required for every transfer of data. However, obtaining the consent of all policyholders is not only time-consuming and expensive. It is also not feasible in most cases since experience has shown

that the majority of the data subjects simply do not respond to the request to give their consent. Given the necessary changes of business processes, it is impossible to ask each individual policyholder for consent every time. Thus, ultimately, the question arises as to whether or not a consent is appropriate for areas which imperatively require data uses. It would be more appropriate to create a legitimate ground for these cases.

b. Information and transparency The German insurance industry endorses the inclusion of information requirements, as already rudimentarily provided for in Article 8 of Convention 108. Only if the controller, the purposes of processing, their own rights of access and of rectification are known to them, data subjects may decide autonomously on the use of their data. Accordingly, the prerequisite of being informed does not only concern data uses requiring consent. For the information of data subjects, Articles 10, 11 and 12 of the Directive 95/46/EC provide for a solution which meets the interests of all parties involved and provides for good access to the data recorded. For the insurance industry, there is an additional special regulation in the German Insurance Contract Act on the collection of health data from third parties, which provides for the obtention of consent, information duties and a possibility of objection. This system of regulations is consistent in itself and has proven its worth in practice. If the two-tier system of general information/notification, including the possibility to require more detailed information, is used, data subjects are not overwhelmed with information. However, they are provided with any essential information which enables them to learn more. Those who wish so will then be provided with detailed information, those who do not are spared from this.

11. Special categories of data

In most cases, biological or biometric data, in other words genetic data, are already health data and therefore especially protected by Article 6 of the Convention 108 anyway. For biometric and genetic data it has to be ensured by clear definitions that for instance sex and age, i.e. characteristics which are visible for everybody, do not come under these. Only data which are obtained at the level of DNA, RNA and at chromosome level should be covered.

Other data should only be subject to the strict safeguards if they are actually comparably sensitive. This does not apply to national identification numbers because these have no sensitive content, which would involve greater protection requirements. The restrictive requirements in Germany with regard to the collection and processing of the tax identification number are due to reasons of constitutional law. However, in this respect, there are differences between different states (cf., for instance, the Scandinavian states).

12. Children

The main objective should be to strengthen the media competence and data protection awareness of minors, especially if these are active on the Internet – in social networks, blogs and chats – and disclose information there. The introduction of a rigid age limit, as considered for the review of Directive 95/46/EC, is not very helpful because in most cases parents or other legal representatives have no sufficient overview and possibilities of control over the action of minors and also because any indication of age, for instance by the network operator, cannot be sufficiently verified. For the offline world and as far as contracts are concluded on the Internet, an age limit of 18 years seems appropriate, inter alia, to ensure conformity with regulations of contract law. If parents conclude an insurance contract for their child, the collection and processing of the data which are required for the proper initiation, fulfilment and settlement of the contract must remain possible.

13. Data security breaches

Obligations to inform if data breaches occur, such as provided for by the e- Privacy Directive, can be helpful to data subjects and can also induce controllers to act carefully. Within the scope of the most recent amendment of German data protection legislation in 2009, Sect. 42a *BDSG* also introduced a duty to furnish information in the case of unlawful gaining knowledge of data. This obligation applies if especially sensitive data are affected and if there is a risk of severe impairment of the rights or legitimate interests of the data subject. As far as we know, German data protection authorities have so far gathered positive experience with this rule. It is applied only if there is actually a serious risk.

By contrast, the duty of information according to the E-Privacy Directive provides that the data protection authority has to be notified of all data protection breaches. The authority may adopt guidelines and give instructions with respect to the circumstances under which notification is required as well as with respect to the format and the procedure of notification. Experience has shown that due to the competence of the data protection authorities of the federal states for the non-public sector this would lead to different rules in the different federal states to which insurance companies operating throughout Germany would have to adjust.

In order not to bother customers and to avoid an effect of desensitisation caused by too many cases of application, it would be appropriate to restrict the obligation to inform in the case of data breaches to situations in which there is actually a risk for the data subject. For instance, a future provision might only interfere if particularly sensitive data are affected and if there is a risk of severe impairment of the rights or legitimate interests of the data subject. It is reasonable to first provide for the reporting to the authority and to decide subsequently whether and how the data subject has to be informed. Moreover, it has to be ensured that the information must not be used at the expense of the data subject in criminal proceedings or administrative offences proceedings.

14.-15. ./.

16. Privacy by design

When introducing new technologies, every company has to ensure that these are consistent with data protection standards. In this respect, the focus should be on the objective to design programs and procedures in such a way as to ensure that data security is ensured. Privacy by design should be reflected in Convention 108 as a general principle. It should not mean that any data protection going beyond existing data protection law is required because this would put an enormous cost burden especially on small companies, which would ultimately be squeezed out of the market.

17. Right of access A right to know the source of data is relevant to the area of advertising where data are disclosed repeatedly and where it is no longer possible to identify the body which originally collected the data. In this respect, the German legislator took the initiative by stipulating an obligation to record the information on the source of data and the recipients during a period of two years (Sect. 34, para. 1a *BDSG*). So far, this obligation has worked well in practice. The question concerning access to the logic of the processing should be explained in more detail.

18. Right of opposition / right of oblivion

Contrary to what is set out in Question 18, the insurance industry considers a right of opposition not to be generally justified where the data processing is not based on the data subject's consent. Within the scope of Directive 95/46/EC, the legitimate grounds according to Articles 7 and 8 may form the basis of legitimacy as well. If this is the case, no general right of opposition may apply.

If contracts have been concluded which require the processing of data to a certain extent, like for instance insurance contracts, these data must be available for the conclusion and fulfilment of the contract. Also, for this reason, a right of oblivion, in other words a "right to be forgotten" may only be envisaged if at all, in connection with the use of social networks on the Internet, but not for the offline world. Therefore, rules for better enforcement of requests for erasure would be desirable. Legal duties to preserve records, such as according to regulations of commercial and tax law, must remain unaffected.

19.-22. ./.

23. Class action and alternative dispute resolution

A possibility of class action is only appropriate where national data protection authorities do not exist and where there are no other protective mechanisms either. Within the scope of Directive 95/46/EC, according to Article 28, use is to be made of supervisory authorities the extensive powers of which are to be further strengthened within the scope of the review of the Directive 95/46/EC. They may act not only upon request of the data subject but also ex officio. Recently, the powers of the data protection authorities have been extended significantly in German law, so that there is no protection gap. In the offline area, instead, out-of-court possibilities for dispute settlement should be developed as a matter of priority. For instance, the German insurance industry has gathered positive experience with its ombudsman for insurance1. The ombudsman is a neutral and independent arbitration board, which works free of charge for the consumer and enjoys wide acceptance among customers (in 2009, more than 18 000 cases have been accepted and concluded). It has proven its worth as an institution which is inexpensive and easily accessible to customers. It would be recommendable to use existing arbitration boards such as the ombudsman also for the area of data protection.

24. Rule determining the applicable law

The German insurance industry welcomes the objective of adding a rule on applicable law to ensure more legal certainty. The existing country of origin principle for cross-border movement of data within the EU (reverse conclusion from Article 4 (1) (a) of Directive 95/46/EC) should not be excluded by a requirement.

25.-27. ./.

28. Internationally agreed minimum standards

The German insurance industry welcomes the intention to create international minimum data protection standards because in states without any data protection these rules may help raise

public awareness of data protecton and establish a basic data protection level. Moreover, in states with a low degree of data protection, the data protection level may be raised in this way. 1 More at www.versicherungsombudsmann.de

29. Binding Corporate Rules

Already according to Directive 95/46/EC, the stipulation of BCR is a way to legitimize international data flows. An important aspect is the practicability of authorization procedures. This includes recognition of the authorization granted by one data protection authority by other authorities to avoid multiple cost-intensive and time-consumung inspection effort.

30. ./.

GERMANY – FEDERAL GOVERNMENT

Comment of the Federal Government regarding the modernization of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

The Federal Government is convinced that Convention 108 and its principles have proved satisfactory in the 30 years of their application and contributed significantly to ensuring data privacy in Europe and in non-European countries.

In an increasingly globalized world and highly complex information societies, data protection requirements have changed over the years. Therefore, the Federal Government welcomes the initiative to revise Convention 108 and to identify parts that may require modernization and adjustments to meet new challenges and needs.

However, if the Convention is amended, its general nature should be preserved. The current purpose of the Convention, i.e. to provide a fundamental, general set of data protection rules, has proved adequate in practice. So far, there has been no place in the Convention for highly differentiated, detailed rules. In the opinion of the Federal Government this principle should be maintained in the future.

In particular, it does not seem useful for the Council of Europe to draw up a set of rules as specific as those envisaged at EU level. At best, such a set of rules would compete with those to be adopted at EU level, and at worst, they would be incompatible.

The Federal Government believes that a general set of rules with clear and comprehensible provisions offers the best chances to convince other States to accede to Convention 108. This, in return, would strengthen the global reach of the Convention. The following should be noted: The more detailed the legislation, the greater the need to take account of the specificities of individual areas, such as police and judicial cooperation.

The Federal Government is willing to help with this important task of modernizing Convention 108.

The Federal Government will comment separately on the questions raised in the consultation procedure of the Council of Europe in January 2011.

GS1 IN EUROPE

GS1 Response to the Consultation on the Modernisation of the Convention for the Protection of Individuals with regards to the Automatic Processing of Personal Data (Convention 108) of the Council of Europe

GS1 would like to thank the Council of Europe for the opportunity to comment in the consultation process on the modernisation of the Convention 108 for the Protection of Individuals with regards to Automatic Processing of Personal Data.

We note that the modernisation of the Convention occurs at the same time as the revision of the European Commission's Directive 95/46/EC on Data Protection and we believe that these two initiatives create the potential for the development of a coherent and harmonised framework of legislations and recommendations.

GS1 has engaged at the EU level in the privacy debate in the framework of our work on RFID and the Internet of Things. Therefore we will focus our comments on those questions that are linked with our experience in the development of a Framework for a Privacy Impact Assessment (PIA) for RFID Applications which was called for in the European Commission Recommendation *on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.*[1]

We hope through our comments to help the Council find the most effective and efficient means to accomplish the widely shared goals of protecting the privacy of personal data while ensuring the free flow of information between peoples and the promotion of innovation.

Object and scope of the Convention, Definitions

Based on the debate over specific technologies in the past, including RFID technology, we believe, with regard to question 1, that a technology neutral policy is crucial in order to foster innovation while providing the protection sought by the Convention.

To take the example of one particular technological development - the emergence of the Internet of Things (IoT) - we are not entirely confident that all of its implications for the traditional means of protecting privacy and security have been fully appreciated. While IoT is sometimes misunderstood just to refer to RFID and other means of object identification, the more lasting impact may come from the rise of sensor networks. Predictions of the growth of networked sensors anticipate billions of autonomous and semi autonomous sensors in our environment in the foreseeable future. It is difficult to anticipate how the existing mechanisms of notice and choice, for example, both being based on sound principles for privacy protection, would apply to many forms of sensor networks. Other principles, such as access, do not easily map to the

[1] Commission of the European Communities, 12 May 2009, C (2009) 3200, http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

development of the IoT and some effort will need to be made to determine how such important principles can be supported while realising the substantial benefits that the IoT can bring. We would recommend that the Council engage in a more in-depth examination of the relationship between the requirements of the Convention and the development of the Internet of Things if a revised Convention is to be effective in the years to come. One possibility to consider is to place necessary exchanges of data between sensors/devices outside the scope of any revised Convention until such an examination takes place. In any case, history has taught us that a focus on enduring principles, such as those that underlie this Convention, and a regime that permits flexibility and encourages innovative, efficient, and effective actions to further those principles, is far preferable to one that sets in place inflexible, immutable and increasingly prescriptive rules.

An additional point we would like to raise relates to the definition of personal data. A tendency of which we became aware during the development of the PIA Framework for RFID Applications was the potential expansion of the types of data that would fall into the category of "personal data". Some have argued for a definition of personal data that would include any information that *could* be linked to an individual or an identifiable person. If the definition of personal data information becomes, either by law or practice, equated with any data that *could* potentially be linked, the definition would sweep in almost all data dramatically increasing burdens on all and diluting the focus on those risks to privacy that may have the most significant consequences.

Protection Principles

In relation to question 7 and 8, while we recognise the importance of the issue raised, we would like to highlight the challenge that could emerge from applying this principle to the Internet of Things. Imagine, for example, a sensor network used to monitor electricity use in buildings such as hotels for purposes of energy conservation. What forms of notice and consent would be appropriate? Similarly, how should data minimisation requirements apply? As Paul Schwartz has recently pointed out, data minimisation requirements may well be at odds with even the most ethical data analytic practices which depend on increasing rather than decreasing the amount of data to be analysed to find relevant and sometimes unanticipated connections.[2]

In question 14 the Council asks about the need for special rules regarding "localisation" data. Such data can take many forms and must be analysed in context to determine the risk, if any, that result from its use. Any rules must recognise the variations in such data and the contextual nature of its gathering and use if innovation is to be encouraged while privacy is protected.

The third point we would like to address regards accountability mechanisms (Question 15). Privacy discussions often take place in the abstract with too little attention paid to what actually occurs within organisations. We believe that those closest to and most directly affected by a decision on an issue should take a leading role in addressing the issue. In the case of the proposed PIA Framework for RFID Applications, this was accomplished by having industry develop the Framework utilising a broad outreach to interested parties.

[2] Data Protection Law and the Ethical Use of Analytics by Paul M. Schwartz, the Centre for Information Policy Leadership, Hunton & Williams LLP, Washington DC 2010 http://www.huntonfiles.com/files/webupload/CIPL_Ethical_Undperinnings_of_Analytics_Paper.pdf

More generally, we would like to offer the following recommendations in relation to:

The role of self-regulation as exemplified in the development of the PIA Framework for RFID applications

The nature of the development process of the PIA Framework for RFID Applications inevitably involved larger enterprises with full time specialised staff dedicated to public policy issues, as well as associations that represent broad industry segments. Even with the best of intentions, small and medium-sized enterprises that bring extraordinary vigour to the marketplace are less likely to contribute the staff time needed to participate directly in such policy processes. The result is that what emerge from these policy processes are solutions less likely to reflect the particular conditions and needs of individual small and medium-sized enterprises. We endeavoured in the PIA Framework for RFID Applications to ascertain and reflect the needs of small and medium-sized enterprises, and we strongly believe that any proposed changes in the Convention should be evaluated based on their impact on these sectors.

A corollary to this point is that public policy, by its nature, often creates "one size fits all" requirements. It is nearly impossible to customise public policy requirements. In discussions leading to the development of the framework, we learned about the wide range of differences among the entities that we represent in terms of their understanding of privacy and security issues, in resources that they can devote to these issues, and in their technical sophistication. In light of this, any future changes in the Data Protection legislation should focus on the aims to be accomplished rather than on specifying the use of a particular means to accomplish them. Such a focus would recognise the variety of entities affected and the differences among them, and would allow them greater choice in deciding how to most effectively and efficiently accomplish the stated aims. This would provide entities both large and small with the opportunity to innovate in finding public policy solutions just as they innovate to meet customer needs. A combination of allowing greater flexibility in the choice of means, acceptance by entities of greater accountability, and enforcement directed at inappropriate actions such as improper use of data is likely to be more successful in accomplishing the goal of effective compliance than continually increasing prescriptive requirements. We believe that a focus on fundamental principles, and the provision for flexibility in achieving them, have been major contributors to the success of the present regime and are even more necessary in today's rapidly changing technological environment.

This Industry led effort to develop a Privacy Impact Assessment Framework has been officially endorsed by the Article 29 Working party, representing the national Data Protection Authorities at European level, in February 2011, showing a wide support for this initiative based on the importance of self regulation.

The Importance of Analysing Threats and Crafting Proportionate Safeguards

It is far easier, less costly and less time consuming to enumerate steps that entities should take to protect privacy and security than it is to implement them. Considerable care needs to be taken so that privacy and security issues are identified, potential threats are rigorously analysed, actions taken to address the threats are proportional to the risk and magnitude of the threats,

and any burdens are minimised so as not to discourage innovation that is based on the gathering and use of data.

In the process of creating the framework we attempted to better understand the various potential threats to privacy and security. This was an important exercise which is now included in the PIA framework itself. However, at the same time we came to recognise that too often there is a tendency to treat all threats as if they were equally likely or equally consequential. In response to question 7 of the consultation on proportionality, we recommend that the Council place the greatest emphasis on identifying those threats which are the most likely to occur and which are most likely to have the most damaging consequences. Resources, whether in money, or attention, are in short supply. It is no doubt necessary to be inclusive in identifying threats, but it is also important to analyse each threat's likelihood and gravity in order to employ limited resources in the most efficient manner in crafting proportionate safeguards that deal with the most serious threats.

With regards to the principle of privacy by design, we believe that it should be viewed in the context of self regulation. Based on our experience in the development of the framework for RFID, we believe that the increased use of PIAs will encourage privacy by design and help foster a heightened awareness throughout organisations of the need to take into account issues of privacy and security. PIAs can increase the accountability that should be a central part of any long lasting and effective framework. But PIAs are not the complete answer for achieving the Council's goals. Because of the extensive resources which PIAs demand, they should be required only in specific and limited cases where the threats to privacy and security are both likely and serious.

Rights – Obligations

In question 17 the Council asks if the right of access should extend to the logic of the processing. Such an extension carries with it the potential for a substantial expansion of administrative burdens and expense and provides little if any additional benefit. It would also raise serious questions about the disclosure of confidential business information and processes.

With regards to the potential introduction of a "right not to be tracked" as referred to in question 20, we would like to reinforce our observation on the risks to innovation, particularly by imposing prescriptive rules in the early phases of development of emerging technologies. Slogans provide little guidance and tend to expand so we would encourage the Convention to continue its focus on clarification and improved effectiveness and the identification of the most significant risks and resist endorsement of any new "right" without an in-depth understanding of the implications for users and industry.

Sanctions and Remedies

We would hope that the Council would look beyond prescriptive measures as suggested in question 23 but would also solicit, and welcome, mechanisms that would provide more positive incentives for appropriate treatment of data in the Convention.

We already have in place strong positive incentives to treat data appropriately if we are to keep the trust and respect of our customers and there are strong negative incentives that exist due to the potential for enforcement actions. There may well be other positive incentives that could play a helpful role in the system as a whole. It may be possible to consider, for example, a gradual reduction of administrative requirements based on an entity's record of compliance or of their having exceeded privacy and security requirements. This arrangement would be in a form analogous to providing procurement incentives for builders who achieve increasing levels of sustainable construction.

The issue of incentives should also play a part when considering the possibility of providing standardised forms that might be used to fulfil, for example, privacy notice requirements. There is much to be said in favour of clarifying requirements and creating safe harbours via the use of standardised forms. But some attention should be paid to ways in which entities could innovate as to improve these forms; standardisation may inhibit innovation as well as foster it.

Transborder Data flows

We believe the Convention should reflect the growing importance of harmonisation of privacy and security requirements across the market and the creation of a level playing field for all parties. The Council has wisely recognised this need in its questions regarding data protection authorities and transborder data flows. Even in the process of fulfilling the Commission's request for the development of a common PIA Framework for RFID Applications we were unable to determine in advance how a PIA might be treated by the data protection authorities of individual Member States. The potential for multiple, burdensome, and even unnecessary filings or disparate treatment across the Member States is a source of considerable concern, particularly for entities that do business in a number of these States. **It is critical for the Convention to encourage an integrated approach, both within Europe and globally, and to minimize administrative burdens in order to increase compliance.**

As an international organisation, GS1 must emphasise the need for harmonised or easily interoperable data protection rules that operate smoothly at a global level. That is the level at which many of the users of our standards operate and the level at which commerce increasingly operates. **We cannot stress strongly enough the need for global agreement on privacy principles, practices, and processes before any new requirements are put in place.**

INTERNATIONAL JOURNAL OF COMPUTER LAW, SECURITY REVIEW, THE INTERNATIONAL ASSOCIATION OF IT LAWYERS, ILAWS, UNIVERSITY OF SOUTHAMPTON

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (generally referred to as “Convention 108”), enacted in 1981, is the only legally binding international treaty dealing with privacy and data protection. The Convention provided the legal framework for the EU Data Protection Directive 95/46.

When Convention 108 was drafted, the computer world was very different to the one which we inhabit today. The Convention was designed to regulate what was in many respects a niche activity. Today, it is difficult to identify any activity which does not involve interaction with computer-based technology. Developments with contact-less debit cards and the inclusion of payment facilities in mobile phones are bringing even the most basic transactions, such as the purchase of a cup of coffee, into the data processing and protection arena.

There is little in the data protection principles with which anyone could disagree. Application is another matter and 30 years on the prime task for revision of the Convention should be to make the instrument the basis for global consensus regarding the manner in which personal data should be processed.
There appears to be widespread recognition within Europe that significant reforms to data protection law are overdue. In this regard, reference can be made to the review commissioned by the UK's Information Commissioner and published in 2009 and to the consultation launched by the European Commission in 2010.
With new data protection challenges arising every day, the Convention is being overhauled to meet new realities. The review aims at 'modernising' the Convention without altering its basic principles, but looking at adding new ones such as those of proportionality and privacy by design. Pursuant to the Notice Published by the Expert Committee under Convention 108, the Computer Law and Security Review, the International Association of IT Lawyers and the Institute for Law and the Web (ILAWS) at the University of Southampton welcomes the opportunity to submit the following comments:

CLSR
Computer Law and Security Review (www.elsevier.com/locate/clsr), an international journal of technology law and practice edited by Prof Steve Saxby of Southampton University since 1985, provides a major platform for publication of high quality research, policy and legal analysis within the field of IT law and computer security and is available on ScienceDirectTM http://www.sciencedirect.com/, the world's foremost provider of electronic scientific information to more than 12 million subscribers.

IAITL
The *International Association of IT Lawyers* (IAITL) is an international association constituted primarily of lawyers and legal practitioners who have an interest in IT law. The IAITL seeks to promote study and research in the field through international conferences, networking, publication of member’s research works, job announcements and the provision of internet resources.

ILAWS
ILAWS is the *Institute for Law and the Web* (http://www.soton.ac.uk/ilaws/) at Southampton University. It was established in 2006 to work on the legal issues, problems and opportunities

associated with the Internet, the Web and digital technology. It is a unique interdisciplinary research centre that combines legal expertise in key domains such as IT law, e-commerce, and intellectual property law. CLSR, IAITL and ILAWS appreciate this opportunity to provide comments structured around the questions posed in the Consultation Document.

COMMENTS

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

Submission: The Convention should remain a simple, concise and technologically neutral instrument, while at the same time recognising and addressing some new characteristics of the present and future technological environment, in ways which we explain below.

Traditionally there has been a reluctance to provide a legal definition of a computer but given the all pervasive nature of the technology this does need to be attempted, perhaps in terms of establishing a de minimus limit.

Whilst context is important and so, for example, a list of 100 target mobile phone numbers in the hands of a private detective might have significant impact upon the individuals concerned, this can be regulated under general criminal law principles rather than data protection rules. The task is not a simple one and the principles of technological neutrality have value. Legal progress, however, should not be neutered by technology. A situation where hundreds of millions of mobile phones come within the legislation ,but where there is no realistic prospect of enforcement can only bring the underlying legal concepts into disrepute.

2. Should Convention 108 give a definition of the **right to data protection** and **privacy**?

Submission: No. It would not be helpful to try to define the right to privacy in a data protection Convention – it is a set of interests which manifest themselves in different ways in different contexts, and sometimes need to be balanced against other interests. It is more appropriate to express them as a set of broad principles. There are other instruments such as the European Convention on Human Rights, and the case law interpreting it, where broad statements of privacy protection are appropriate, and different mechanisms used for enforcement.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Submission: Yes, it is important that the Convention and its principles apply broadly – any areas in which derogations from some principles may be justified need to be specific and focussed.

4. Convention 108 does not exclude from its scope data processed by a natural person in the course of a purely

personal or household activity. Should this continue to be the case or should a specific exception be

introduced (and specifically considered in the context of Web 2.0.)?

Submission: This is a difficult issue – full application of privacy principles to the behaviour of private individuals would be onerous and oppressive – threatening other important freedoms and rights. But modern technology increasingly allows individuals to threaten the privacy of others in ways that were previously only available to organisations, and some controls and restrictions are therefore justified. This is best handled by a broad statement of privacy protection in the ECHR and similar human rights instruments, at the international level. Some consideration could be given to making the privacy protections in those instruments more specific.

At the national level, the issue is best dealt with by statutorily defined rights of privacy where interpretation by the Courts has a major role.

5. The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?
Submission: The only principle currently applying to collection is in Article 5 – that personal data undergoing automatic processing shall be: (expressly, in (a)) "obtained and processed fairly and lawfully", and (implicitly) that data collected should be "adequate, relevant and not excessive ..." (in (c)) and "accurate" (in (d)). We submit that it would be helpful to include 'collection' in the definition of automatic processing so that all of the principles apply, where relevant, to collection. The principle needs to be strengthened by inclusion of a specific requirement that collection should not be excessive, and perhaps that it should not be by intrusive means. However, the 'data minimisation principle' (see response to Q9) is another way to achieve at least the first objective.

6. The definition of the **controller** of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?
Submission: The definition is satisfactory, criteria are and should be independent and there can be several controllers for one file.
The classic formulation is that a data controller is the entity which controls the extent to which data may be processed. It is based very largely on the precept that data is held in the same manner that a library may be held to control the books on its shelves. This is less relevant in a networked environment with systems of data sharing and matching being used increasingly in both the public and the private sectors. It is becoming increasingly difficult for data subjects to seek a meaningful answer to the question what data a controller might store when the real issue concerns the extent of the data which the controller might access. There can be no perfect answer but where there are formal systems of data sharing or matching there should be a requirement to nominate one entity as having overall responsibility (as is the case with systems of binding corporate rules under the EU data protection directive). There should also be an obligation upon individual data controllers to include in their response to individual subject information requests data relating to formal data matching or sharing networks in which they participate along with details of the coordinating entity.

7. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.
Submission: These new definitions would only be necessary if provisions were inserted referring expressly to these entities. This may be necessary if provisions concerning 'privacy by design' are included, because it is essential that such a principle should apply to those designing technical equipment and not merely those utilising it, as it may be too late to factor in (or retro-fit) appropriate privacy protections once technologies are built without them. (see response to Q17)
See also response to Questions 15 and 21 below concerning the definition of 'personal data'.

Protection principles
8. New principles could be added to the Convention, such as the **proportionality** principle, which should apply to all operations carried out on the data. Such a principle is also linked to the **data minimisation principle** which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.
Submission: These are both significant principles which could valuably be added, and we strongly support their inclusion. At the level of general principles there can be little to object to or criticise in the underlying principles. As always, the devil is in the detail and in some important respects there may be need to update the definition of concepts in order better to meet the needs of modern data processing realities. There has been some discussion recently of the value of establishing a right to be forgotten in respect of online data – that is, people should be able to give informed consent to every site or service that processes their data, and they should also have the right to ask for all of their data to be deleted. If companies don't comply, citizens should be able to sue. This is a topic

which might benefit from expansion of the existing requirement that data shall not be retained for longer than is necessary for the purposes for which it was first processed. Given our increasingly networked world there will be obvious difficulties in ensuring compliance with such an obligation but there might be merit in requiring the original processor to inform the data subject of the period for which data will be retained by them. In the case of a social networking website, it might be feasible to indicate that members will be contacted after 2 years with the request that they confirm whether they wish their details be retained. There might be debate whether an opt in or opt out approach would be preferable. The advantage of the former approach is that many users may have changed emails and forgotten about the existence of a page.

9. Should the question of **consent** be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?
Submission: The concept of consent is fraught with difficulty in a data protection context. If it is used, it needs to be expressly defined as meaning free, voluntary, informed and revocable at any time, and not bundled with other consents. Effective consent requires comprehensive information about the range and origin of linked data, the purpose of the profile and how it will be used, the controller and planned date of deletion. If consent is withdrawn, the profile must be immediately deleted, also by those controllers to which it has been transmitted.

There are many current transactions which misleadingly use 'consent' when they in reality amount only to 'notice, and acknowledgement that nominated uses/disclosures are a condition of the transaction'. There should be a general principle that where genuine consent is a realistic option, it should be the preferred basis of fair processing (subject to other public interest exceptions), consistent with the overall aim of transparency in transactions involving personal data. Specific areas where there might be need for more explicit legislative provision might include the requirements imposed on data controllers to inform subjects of the uses to which data might be put. In the case of social networking sites, for example, this might include clear statements of privacy options and the positive and negative implications of choices which might be made by subjects. Provision might also be made regarding the default settings associated with such sites and data processing general. It might, for example, be provided that a minimal range of access to or dissemination of data should be provided unless and until subjects make an informed choice to extend these.

10. Should the **legitimate processing** be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?
Submission: No – fair and lawful (i.e. not unlawful), coupled with other general principles of proportionality, data minimisation and non-intrusive collection, are appropriate criteria – a list of positive grounds for processing would inevitably be incomplete.

11. Convention 108 does not expressly mention **compatibility in relation to purpose**. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.
Submission: Compatibility is a subjective concept, and would be better expressed as 'uses or disclosures which are within the reasonable expectations of the data subject (to which a 'reasonable person' test would be applied). However, it should be made explicit that 'reasonable expectations' can only encompass uses or disclosures which a reasonable person would consider to be both fair and compatible with the original purpose of collection. Uses and disclosures outside 'reasonable expectations' should only be permitted with (genuine) consent or under a prescribed exception.
The central rules embodying the fairness and purpose specification (finality) principles should be re-worded in order to elucidate their implicit concern for the reasonable expectations of data subjects. More specifically, the rules should be re-formulated to make clear that when information is

collected and processed for a particular purpose, it should not be processed for another purpose that is not within the reasonable expectations of the data subject, unless the latter consents or the re-purposing is either legally authorised or justified by a compelling public interest.

12. **Special categories of data** which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

Submission: Unless the Convention is to specify the additional measures, then there is limited value in defining 'special categories' or 'sensitive data'. Sensitivity is in any case subjective and contextual, and any list is likely to be arbitrary and incomplete. The proposed introduction of proportionality and data minimisation principles (see Q8) could replace the need for a 'special category' provision.

Instead, we suggest a general definition of the term "sensitive data" which are capable by their nature of infringing fundamental freedoms or privacy" and mentioning specific types of data only as examples. If this provision is to specify the additional measures, it should include additional categories of data (such as biological, genetic and biometric data), and future developments of "new data". It should avoid conclusive lists of particular data categories subject to a general prohibition on processing, which can be limited by extensive exceptions.

The Convention should, however, explicitly accept the rights of member states to provide a higher level of protection for data which provides a higher level of risk to privacy interests than other personal data, proportional to that higher risk.

13. A specific protection could also be applied to certain categories of data subjects. In particular, **children** may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

Submission: There is no need for specific protections for certain categories of data subject. The proposed introduction of proportionality and data minimisation principles (see Q8) should adequately address the concerns about children and other potentially vulnerable groups. The explanatory materials accompanying the Convention could make this clear.

14. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Submission: Yes, but not necessarily as part of a security principle – a right for data subjects to be informed of data breaches affecting them that meet specified threshold criteria should stand alone as a separate principle. Data protection principles should encompass the notion of requiring that data subjects whose data may have been mislaid or which may have been made susceptible to unauthorised access should be informed about this possibility and advised as to possible remedial measures. Taken in a specifically UK context and considering in particular the reluctance of the police to volunteer to individuals information that their voice mail services may have been subject to acts of unauthorised access by private detectives working on behalf of journalists, there might be difficulty in determining where notification responsibilities might best be placed. The general principle of imposing breach notification obligations does seem clear.

15. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Submission: There would be no need for separate principles or rules for traffic or location data if personal data is defined as expressly including any information which enables or facilitates communication with a person on an individualised basis, whether or not it meets the current definition of personal data. This would include information about an individual's communications or

location, and would include IP addresses, email address,other communications addresses, and geolocation data. (See also response to Q21 for additional inclusion of 'behaviour' in the definition)
16. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?
Submission: Yes – there should be an obligation to demonstrate that measures have been taken to ensure full respect for data protection rules. Caution should be taken in the use of 'accountability' which has been suggested in recent data protection debates as alternative to specific requirements for compliance with rules. In particular, 'Accountability' cannot be and must not become an alternative to data export restrictions.

17. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?
Submission: Yes, privacy by design should be expressly encouraged. See further the response to Q22.

Rights – Obligations
18. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?
Submission: The right of access should include a right to be informed, on request, of the source of the data, also all recipients of the data (more specific than the general description given in collection notices), and also, where practicable, an explanation of the logic of the processing, e.g. credit scores.

19. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

Submission: A right of opposition in the sense used in the EU Directive (Article 14); i.e. a right to opt out of processing, should be included, even when consent was originally granted, if it is reasonable for consent to be revocable in the circumstances.
A right to oblivion (to be forgotten) needs further consideration, as there may be many circumstances in which it is unreasonable or impractical, and even conflict with other principles such as security or data integrity, or interfere with the audit trail needed for accountability
A 'right to be forgotten' should at the very least encompass a requirement that personal data should be deleted or made inaccessible once the purpose for its collection is complete, though this does not meet all situations where such a right is needed or justifiable.

20. Should there be a right to guarantee the confidentiality and integrity of information systems?
Submission: There can be no absolute guarantee of confidentiality or integrity – only that 'reasonable' measures or steps are taken. Supervisory authorities do, however, need to be much stricter in their enforcement of these principles.
The Convention (and other data protection codes) needs to be supplemented with more detailed rules on the quality of information systems. More specifically, a set of rules should be drawn up stipulating that the development of information systems shall be oriented to maximising – within the boundaries of what is technically feasible and reasonable – the manageability, reliability, robustness, comprehensibility and accessibility of the systems, both from the point of view of systems users and of data subjects. Useful points of departure for the drafting of such rules are the core principles of the OECD Guidelines for the Security of Information Systems. Despite being somewhat prolix and, on their face, only tangentially relevant to data protection concerns, these principles are worth taking note of given the paucity of equivalent principles in data protection codes. The ideas they express should inspire the drafting of a similar set of rules dealing with the

quality of information systems from a data protection perspective. The broad thrust of such rules would be as follows:

a) Information systems shall be designed so as to improve the extent to which they are able to (i) automatically test aspects of the quality of the data/information they process, and (ii) communicate the results of such tests to the data controllers.
b) Data controllers shall issue information quality declarations that describe the means by which the quality of information processed by the controllers has been checked, the results of such tests and any remaining uncertainty about the quality. The declarations shall be handed to the relevant data protection authorities.
c) Formal agreement shall be reached as to (i) which person(s)/organisation(s) is/are directly responsible and liable for the quality of the information in the system concerned and (ii) how this quality is to be monitored.
d) Data processors shall undergo training in order to be made aware of at least the following: (i) the core principles and rules of data protection; (ii) the basic rationale and importance of these principles and rules; (iii) how these principles and rules apply to their own work tasks.
e) Data controllers shall subject their information systems to periodical data protection audits by a competent and independent third party. 2 These shall ascertain strengths and weaknesses in the data

1 Cf. principle 5.9 of the ILO Code of Practice on Protection of Workers' Personal Data (1997) which stipulates: 'Persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role in the application of the principles in this code'. 2 This sort of rule is present in section 9a of Germany's Federal Data Protection Act of 1990 (as amended) ("Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und – programmen und Datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt").

protection measures taken by the controller concerned. The rule should further stipulate conditions for disclosing the audit results to the relevant data protection authorities and the general public.
f) Extending the latter rule, data controllers should be encouraged, if not required, to undertake ex ante assessments of the impact that their planned data-processing operations or planned changes to the information system(s) supporting such operations, might have on data protection interests. This kind of assessment tends to be championed under the name of 'privacy impact assessment'. The latter nomenclature is somewhat misleading as the assessment is intended to evaluate more than the possible effects of planned activity on privacy as such. Ideally, the assessment should be carried out by a competent and independent third party, and its results made public.
Additionally, the central rules embodying the information quality principle should be reviewed to determine whether they adequately and consistently capture the various facets of information quality and the various facets of assuring such quality. Looking at current data protection laws, significant variation exists in terms of the degree of detail with which they formulate the dimensions of information quality. Concomitantly, there is some inconsistency in terms of the terminology they employ to describe these quality dimensions and the sorts of steps to be taken in quality assurance. Overall, these rules appear to have been drafted somewhat haphazardly. It is best to have honest rules; i.e., rules giving reasonable guidance, on their face, about what information quality and assurance of such quality involve. Information quality and quality assurance are both multifaceted. Rules on them should accurately reflect this fact, especially in view of the need for legal certainty on the part of data controllers and in view of the importance of ensuring adequate information quality in an age of increasing electronic interpenetration. This notwithstanding, some caution is vital when formulating requirements for quality assurance. Such requirements have the

potential of generating operating costs for data controllers which are disproportionately high relative to the risk of error causing detriment to the data subjects. Some form of 'reasonable steps' standard is probably most appropriate. At the same time, this standard should not be determined solely or primarily by the needs of data controllers; rather, it should be linked primarily to what is necessary to ensure fair data-processing outcomes for the data subjects. A point of departure for drafting a general rule on information quality could be the following: 'All reasonable steps shall be taken to check and ensure that data are correct, complete, relevant and not misleading in relation to what they are intended to describe and in relation to the purposes for which they are processed. In assessing what is reasonable, primary regard shall be given to the extent to which data-processing error can have detrimental consequences for the data subject(s).'

21. Should a right 'not to be tracked' (RFID tags) be introduced?
Submission: There is no need for a separate 'right not to be tracked', if personal data is defined as expressly including information about an individual's communications, location or behaviour (See response to Q15)

22. Should everyone have a right to remain anonymous when using information and communication technologies?
Submission: An absolute right to anonymity is unreasonable and impracticable in many circumstances. Consideration should nonetheless be given to including more explicit and systems-active provisions on anonymity. Opportunities for anonymity should be promoted more obviously in the rules embodying the minimality principle. Indeed, allowance for anonymity should be made a basic data protection principle in itself. A principle similar to that already included in the Australian data protection law as the 'anonymity principle'3 could be included. Suggested wording: "Individuals must have the option of not identifying themselves when dealing with an entity, or of using a pseudonym, except where there is either a legal requirement for identification or where it is impracticable for the entity to deal with individuals who have not identified themselves or who use a pseudonym."

3 See NPP 8 in Schedule 3 to Australia's federal Privacy Act ("Wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering transactions") and IPP 8 in Schedule 1 to the Information Privacy Act 2000of the Australian State of Victoria ("Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation"

At the same time, however, the Convention should additionally be infused with provisions explicitly addressing the need to develop organisational-technological infrastructures that promote transactional anonymity. A useful model provision in this regard is s 3a of Germany's Federal Data Protection Act ("Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht"). What is fairly unique about this provision4 is that it explicitly addresses the need to design information systems and other technological platforms to support the goal of minimality. This characteristic ought to be emulated in the Convention. This relates closely to the question of whether privacy-enhancing technologies (PETs) ought to receive greater legal support and if so, how. The answer is yes they do need such support and the rules on point can be easily formulated without breaking regulatory principles on technology-neutrality etc. The rules could be formulated so that they primarily stipulate the goals to be reached (e.g., of anonymity and/or pseudonymity), and their specification of the means for reaching these goals (e.g., in terms of systems development) could be done without singling out and promoting a specific PET.

Following on from the latter points, it is desirable that rules promoting anonymity be supplemented by rules promoting pseudonymity. The appropriate rules should stipulate anonymity as the primary option with pseudonymity as the first fall-back option when anonymity cannot be achieved for legal or technical reasons.
The above proposals should be augmented by rules dealing specifically with profiling. One such rule should be along the lines of § 21 in Norway's Personal Data Act which lays down a duty on the part of a data controller to supply a person with certain types of information about a profile when it (the profile) is used to establish contact with or make a decision about the person. The provision does not require notification of the logic or assumptions behind the profile concerned; nor does it specify the time frame in which the information is to be provided. New rules modelled on § 21 should correct the latter omission by specifying that the information be supplied at the time contact with the person is made. They should additionally require notification of the logic or assumptions behind the profile, at least when it is used to ground a decision significantly affecting the person's rights or interests. The new rules should also make clear that the duty they lay down applies not just in relation to specific profiles but also abstract profiles. The introduction of a duty of information along the lines drawn here will also involve a duty on the part of data controllers to document the profiles and the logic used to generate them.
The traditional definition of 'personal data' should be made more flexible by supplementing the identifiability criterion with a contactability/reachability criterion. More specifically, 'personal data' would be defined as data that facilitate either identification of a particular individual or contact to be made with him/her. This strategy might well prove useful in an Internet context where there is uncertainty as to whether, say, a machine address is 'personal data', yet where the person(s) using the address are subjected to profiling or to measures instituted on the basis of profiling.

23. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?
Submission: It is not appropriate for the Convention itself to try to balance every aspect of these interests, but some recognition of the public interest in freedom of expression would be desirable.

Sanctions and Remedies
24. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?
Submission: The Convention does not currently expressly provide for complaints about breaches of the principles/rules – only for remedies where requests for correction etc are denied (Article 8(d)). If the Convention is to include a requirement for complaint or ADR mechanisms, then it would be appropriate for it to expressly recognise the value of representative complaints (class actions).

4 There is some trace of it also in recital 30 of the preamble to EU Directive 2002/58 ("Systems for the provision of
electronic communications networks and services should be designed to limit the amount of personal data necessary to a
strict minimum").
5 Cf § 21 of the Norwegian Act which creates a duty to provide information about a profiling practice i.e. when a person is
contacted on the basis of the profile.

Data protection applicable law
25. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Submission: There may be more than one applicable law – both general and sectoral data protection laws and other laws with privacy related provisions. Insofar as data protection laws are concerned, it would be of value if, in relation to likely areas of conflict of laws, the Convention did state a choice of law rule.

Data Protection Authorities

26. How to guarantee their independence and ensure an international cooperation between national authorities

Submission: Supervisory authorities are only provided for expressly in the 2001 Additional Protocol to the Convention (CETS 181), and these provisions could usefully be incorporated in the Convention itself (see response to Q26 below). Clause 3 of Article 1 of the Protocol mandates independence, while Clause 5 requires international co-operation. It is probably not appropriate for the Convention to try to specify how these requirements are to be met.

We welcome the intention of strengthening and clarifying the status and powers of the data protection authorities and to fully implement the concept of 'complete independence'. National authorities are notoriously understaffed. To be effective they must have the resources as well as the powers to do their job.

27. Should their role and tasks be specified?

Submission: Article 1 of the Additional Protocol (CETS 181, 2001) specifies roles and functions of supervisory authorities. This should be incorporated in the Convention itself.

One particular task of a supervisory authority that needs to be spelled out is the obligation to account for their performance of their complaint investigation obligations, including by reporting to the public, on objectively determined criteria, of cases investigated (anonymised to the extent necessary to protect privacy but not otherwise), and by statistics including statistics concerning outcomes and remedies. Supervisory authorities must be able to demonstrate that they deliver remedies to complainants; otherwise their existence can simply be a cover for expanded surveillance activities.

The establishment of dedicated supervisory authorities has become a key component of European notions of data protection. In most countries, a single agency has been established. This does perhaps raise an initial

issue. If an organisation is subject to review by another regulator such as one operating in the financial services sector there may be an undesirable element of overlap if it is also subject to the data protection authorities. Just as the European data protection Directive sanctions the establishment of independent data protection supervisors within undertakings as serving to exempt that body from some elements of the normal supervisory regime, so the role for sectoral supervisory authorities whose remit extends beyond data protection might be considered.

Alongside supervisory agencies, systems of licensing/registration/notification have become a key component of legislation. The time may have come to consider whether they serve any useful purpose. Cross reference might be made to the regulation of telecommunications in the EU where established systems requiring prior authorisation have been swept away and replaced by ex post regulatory schema. There may well be data processing systems whose potential and intended impact on society might require some system of prior assessment, but it is not clear that the current systems of near universal registration offer benefits commensurate with the cost implications for both data controllers and the supervisory authority. A much more

focused approach is required to avoid the danger that a disproportionate amount of the supervisory agency's resources are expended in ensuring that controllers have ticked the most appropriate boxes.

In line with approaches in telecommunications regulation, the vast proportion of data controllers should, whilst remaining subject to the requirement to comply with substantive legislative requirements, be exempted from the procedural burdens associated with notification. Apart from

the suspicion that many controllers may not have notified details of their processing activities to the supervisory authority, it is difficult to see what value there is for the public in having a register of data processing activities. If a subject knows of a particular activity, there will be no need to consult a register. If they do not know, such registers will offer little practical help in determining who processes the subject's personal data and for what purpose. The only practical value of notification in countries such as the United Kingdom is as providing the only significant source of revenue to the supervisory authority. Again, lessons might usefully be learned from recent reforms introduced into the European telecommunications legislation which impose an obligation on Member States to ensure that regulatory agencie sare adequately resourced in terms both of financial and human resources. The latter point may be of significance in many instances. Criticisms have been made that the staff of supervisory have lacked the technical knowledge necessary to investigate activities such as the acquisition of large amounts of personal data by Google in the course of its Street Views project. Again, whilst there is a case for making those whose processing activities are capable of impacting on large numbers of data subjects or which relate to sensitive data, it is difficult to justify the imposition of what is effectively a tax on computer users. Again borrowing from the telecommunications sector, charges for the services provided by supervisory agencies should be proportionate to the costs incurred and benefits provided. For the majority of data controllers, it is unclear that costs are incurred by supervisory agencies or that any benefit is obtained by the controller.

Transborder data flows

28. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

Submission: It remains appropriate to require an adequate level of protection as a condition of cross-border transfer. Member states of the Convention should require that the personal data concerning their citizens is protected if it leaves their jurisdiction. The provisions of the additional protocol should be moved inside the Convention.

The Convention (and the European Directive) provide as a start point to their provisions on data transfers outside Member States that these are automatically sanctioned only if the recipient state will ensure an adequate level of protection. In spite of the mechanism for making findings of adequacy under the Directive, few states of any size or significance have been acclaimed as ensuring adequacy.

A dictionary definition of adequacy refers to notions of acceptability or basic fitness for purpose. Many of the Decisions reached by the European Commission on the issue of adequacy seem to require something closer to equivalence. This may be of considerable significance. A Volkswagen Golf is an adequate motor car but it probably would not be considered equivalent to a Rolls Royce. A more precise definitional approach in a revised Convention might make the process more transparent than is currently the case and could serve as a spur for the development of widely accepted standards of data protection. The Convention affords states the possibility of applying higher standards internally and this should be maintained. The current approach towards transborder data flows is not working. The early English/Danish King, Canute, is famous for commanding the incoming sea tide to go back – and getting his feet wet as a consequence. The tale is generally held to depict the vanity and stupidity of the King. An alternative and perhaps more plausible interpretation is that he was trying to show over-deferential courtiers that he was not all powerful. On this account, the folly lay in those seeking to impose controls on forces which could not be mastered. In our networked world, there are limits to the extent to which data flows can be (as has been discovered by states such as Egypt and Tunisia) or should be controlled.

The current European approaches towards transborder data flows are not working effectively. They are burdensome to those whose motives are benign and ineffective towards those more malignly inclined. Problems are, of course, exacerbated by widely differing national approaches towards the

regulation of transborder data flows. Whilst some states require prior approval, others have systems of notification whilst others have no ex ante controls whatsoever. These matters could certainly be addressed with more precision in a revised Convention, but the basic problem is perhaps that legislative structures designed for an era of standalone mainframe computers struggles to cope in a networked environment. A prime focus of any revision of Convention 108 should be to make it a more attractive instrument for ratification by non Member States.

29. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?
Submission: 'Globalisation' of 'minimum rules' is not desirable at all. It would simply be a 'race to the bottom' which would destroy any value in cross-border privacy protection. The Convention should establish the standard of protection it requires for citizens of member states, and adhere to that.

30. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?
Submission: The same basic principle of cross border transfer conditions should apply equally to the public and private sectors.

Role of the consultative committee
31. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it.
Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?
Submission: The monitoring and standard-setting functions of the Consultative Committee should be strengthened.

Conclusion
There is little in the data protection principles that anyone could disagree with. Application is another matter and 30 years on the prime task for revision of the Convention should be to make the instrument the basis for global consensus regarding the manner in which personal data should be processed. The modernisation of the Convention reflects the recognition of the broadening scope of data protection guideline which would enable a universal regulation for Europe and the rest of the world.
We hope that the Expert Committee of the Council of Europe takes in consideration our view and proposals in respect to the modernization of the Convention.

ITALY - GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?
The technologically neutral approach of Convention 108 and its wording as focused on general principles have allowed the safeguards it sets forth to basically stand the test of time. Adjustments are unquestionably necessary in order to take up the challenges arising from the new technological scenarios and globalization; in any case, we would be in favour of sticking to simple, general principles without resorting to detailed provisions that would not be capable to cater adequately to the continued evolution of technology. Furthermore, laying down clear-cut, general principles is in line with the spirit of a Convention that is aimed at attaining basically universal value whilst attracting ratification also from non-CoE countries where no regulatory experience in this area has yet developed.

2. Should Convention 108 give a definition of the right to data protection and privacy?
It would be appropriate for Article 1 of the Convention to explicitly recognise the right to data protection alongside the right to privacy as fundamental rights the Convention seeks to ensure, in accordance with the approach that has been followed (as you well know) by both the Charter of EU Fundamental rights and some national laws.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?
The cross-sector approach of Convention 108 should be retained as it is still valid and has been actually the benchmark for various instruments concerning police co-operation and information exchanges (Europol, Schengen, and more recently the Prüm Treaty). This approach has allowed – as with Recommendation (87)15 – striking the balance between the public interest in preventing/prosecuting crime and the respect of fundamental rights vested in individuals, which has impacted favourably also on fairness and effectiveness of the processing operations performed in the law enforcement area. Additionally, this comprehensive approach of Convention 108 is especially appropriate to the increasingly frequent interactions between public and private bodies in connection with data processing – including the access by public authorities to data collected by private entities. Nor should one overlook the new challenges arising to data protection at European level from the elimination of the pillar-based EU structure brought about by the Lisbon Treaty. Indeed, this is exactly the context where the Council of Europe might play a key role - in particular to define, at international level, the safeguards citizens are entitled to in this area, and thereby contribute to enhancing and improving police co-operation.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?
Generally speaking, the exclusion in question may be appropriate to prevent the exorbitant application of data protection principles to processing operations that do not entail risks to data subjects. However, one should perhaps consider that certain new technologies (like social networks) are making the distinction between processing for exclusively personal purposes vs. other types of processing increasingly blurred. Careful analysis is required prior to introducing the

said distinction; account should also be taken that this distinction is already envisaged in directive 95/46/EC and this topic is being debated as part of the review process of the latter directive.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

Data collection should be included in the definition of processing. Experience has shown that data protection safeguards should apply to all the operations that make up the processing – from its start to its end, including the activities related to use of the data. Indeed, this new definition would be in line not only with directive 95/46, but also with the "International Standards on the Protection of Personal Data and Privacy" approved by the DPAs of 50 countries in Madrid. If additional processing operations are added to the list, this should be done by way of example of a new, much broader "processing" concept.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Generally speaking, when introducing new categories it is fundamental for the definition of the relevant entities to be instrumental to allocating responsibilities and facilitating the exercise of data subjects' rights.

More specifically, given the increasingly complex scenario – partly on account of new technologies and globalization – and the growing recourse to multi-layered organizational structures in both the private and the public sector, adding the definition of data processor may be helpful to take due account of the different roles and responsibilities that are vested in the different stakeholders involved in the processing of personal data. In fact, the need to add this definition was already felt in various CoE's Recommendations (see Recommendation 2002(9) on the processing of data in the insurance sector, and Recommendation 2010(13) on profiling). In this connection, it would be appropriate for the introduction of the data processor definition into the Convention to be coupled with the provision whereby a data controller should always check that data processors provide suitable safeguards in both technical and organizational terms so as to ensure compliance with privacy principles as well as with the instructions given by the data controller. Additionally, it is unquestionably helpful to lay down the safeguards that should be afforded by any additional entities that may take part in the processing on whatever ground – such as the "manufacturer of technical equipment" – whilst the legal obligation to verify the existence of such safeguards should be vested further in the data controller.

<u>Protection principles</u>

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Proportionality and data minimisation are key elements of data protection and could strengthen the safeguards laid down in the Convention. This is shown by the fact that several CoE recommendations on data protection have tried to articulate and elaborate these principles. The principle of purpose-related proportionality should be introduced vis-à-vis every processing operation, partly because of the need to take account of the growing use of new technologies as well as with a view to the possible introduction of the privacy by design principle.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Introducing the principle of consent as a precondition for the processing to be lawful – which actually would be in line with the proposed addition of "collection" to the elements making up the

processing – should take account of the limitations that have been encountered in implementing data protection principles. In particular, one should prevent consent from being relied upon as a legal basis whenever there are marked status differences between data subject and data controller as well as whenever complex processing operations and high-profile technology requirements make it unlikely for consent to be given by data subjects on the basis of adequate information and awareness. New technologies (like the Internet and profiling techniques) highlight the desirability of focusing on other safeguards by preventing consent from becoming a formal, cumbersome requirement that will ultimately prove poorly useful or downright impracticable. At all events, the information provided should always relate not only to processing mechanisms, but above all to the risks arising to data subjects from such processing.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?
As for introducing additional legitimate grounds, it would be appropriate to prevent the principles in the Convention from being modelled too closely after those set forth in directive 95/46 – e.g. because excessively detailed provisions are laid down in the Convention.

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.
Compatibility with the initial purpose is fundamental as a principle and should be introduced into the Convention, especially if one considers the hugely expanded availability of information on the Net with the resulting facilitation in using such information for purposes other than those pursued initially.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?
The data mentioned in Article 6 of the Convention are intended to be protected against their use for discriminatory purposes; they basically mirror the categories protected by international instruments to counter discrimination. The increased protection to be afforded to these data must be left unprejudiced – as actually clarified in the Explanatory Memorandum to the Convention; however, one might envisage a "functional" criterion whereby additional data categories may take on "sensitivity" features because of the context and/or the purposes and/or the mechanisms of their processing, in which case they should be subject to the relevant safeguards. Additionally, one might envisage that these circumstances and data categories may be determined and updated regularly via flexible tools that should not entail amendments to the Convention.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?
Convention 108 may not be the most appropriate instrument to address – in particular – the children issue, which is fraught with many peculiarities that would require specific provisions and thereby subtract from the general nature of the Convention principles.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

The issue of security measures is a key one and the relevant Article in the Convention is certainly to be revised. If one considers recent developments like cloud computing, security can be regarded as actually fundamental. It would be appropriate to also consider whether to expand the "security" concept to include data transmission network security along with the physical security of the places/premises where the data are stored. One might envisage the development of international security standards, which might be helpful to flesh up the privacy-by-design and accountability principles referred to below (see questions 15 and 16). At all events, account should be taken of the ongoing discussion at EU level on security-related issues.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data ?

Location and traffic data fall unquestionably under the scope of the "personal data" concept and are already protected by the safeguards laid down in the Convention. At all events, one might envisage that data categories entailing specific risks to data subjects (such as location data, traffic data as well as databases built up by means of specific technologies) should be subject to the DPA's prior checking.

We would like to point out that it would be desirable for the Explanatory Memorandum to provide examples of the information that is personal data to the extent it relates to individuals that are "identifiable" by the data controller. The Memorandum might actually also refer to sound and image data, as is the case with directive 95/46/EC, and emphasize that the fast-pace development of the information society facilitates identification by data controllers; accordingly, to determine whether a given data is personal data one should take account not only of state-of-the-art technology at the time the processing is performed, but also of the possible (foreseeable) developments over the time span covered by the intended processing. It should also be clarified that there may be many other "identifiers" that go beyond an individual's name and census/behavioural information.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

There is no obstacle to introducing a principle whereby the data controller should take all the measures required to ensure compliance with the principles of the Convention by implementing such internal arrangements as may be necessary to provide proof of compliance to both data subjects and the supervisory authority. The relevant provision(s) should clarify the accountability criteria applying to companies/entities that operate in several countries (see the considerations made concerning question 24 below).

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

These topics are currently being also debated in connection with the review of directive 95/46/EC.

There is no obstacle to introducing the privacy by design principle, which would enhance proactive approaches to protection instead of relying exclusively on remedial measures. However, effectiveness of the principle could only be ensured by specifying how its impact on the specific processing operations can or should be gauged and by whom, in the light of the specific technological arrangements.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?
We think it is appropriate to extend the right of access to the logic of the processing, given the current technological scenario where data aggregation methods (see the profiling issue) are increasingly sophisticated and difficult to grasp whilst they may impact adversely on an individual's private sphere. As regards certain cloud computing-based technologies, one should also envisage introducing the right to know the physical location and the country where the data storage / software distribution servers are located.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.
The specific features of the "right to oblivion" along with its scope are as yet quite controversial and it would appear inappropriate to explicitly provide for and regulate such right in the Convention. Account should also be taken in this regard of the relevant discussion in connection with the review of directive 95/46/EC.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?
Yes (See reply to question 21)

20. Should a right 'not to be tracked' (RFID tags) be introduced?
Yes (See reply to question 21)

21. Should everyone have a right to remain anonymous when using information and communication technologies?
Yes. We would like to point out that – like for questions 19 and 20 – this is in our view where expanding the list of rights and general principles set forth in Convention 108 makes the most sense.
Concerning anonymity, one should ensure that all the processing operations that must be carried out anonymously off-line continue to remain anonymous in the online context. This is obviously without prejudice to the possibility for the competent public authorities to access the data insofar as this is necessary to discharge the respective duties.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?
As for the difficult reconciliation of freedom of expression and private life, we would like to recall the key role of the European Human Rights Court, which has applied the principles set forth in Articles 8 and 10 of the EHRC to issue decisions that take account of the specific features of each case without losing sight of the broader picture. This is why we believe it might be dangerous to add further provisions that might prove less flexible and fail to mirror the mutual interactions of the two principles (as often clearly described in the relevant case law) in an equally balanced manner. As regards the issues related to Web 2.0 - which are relatively new also in terms of case law - laying down specific, ad-hoc rules would appear to be premature.

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

It should be considered that these issues are currently being debated in connection with the review of directive 95/46/EC.
The introduction of class actions would be a major step forward in order to strengthen individuals' rights in a scenario where the available remedies are somewhat unsteady. However, the relevant regulations differ considerably in the individual countries. It might be appropriate to urge States to also make available this remedy, without introducing binding provisions in the Convention.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?
Introducing rules on applicable law would not appear to be desirable. The latter is an overarching issue that has to do with areas at times regulated by binding legislation as well as with sensitive issues in terms of freedom of expression?

Data Protection Authorities
25. How to guarantee their independence and ensure an international cooperation between national authorities? 26. Should their role and tasks be specified?

It should be recalled that the Additional Protocol to the Convention outlines the tasks and independence requirements applying to DPAs quite adequately. As for Chapter 4 of the Convention (concerning mutual assistance between contracting Parties), we think it would be appropriate to better define the co-operation mechanisms between DPAs – possibly by envisaging specific interaction mechanisms and/or joint forums.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.
28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?
It is unquestionably necessary to reconsider the concept of "transborder data flows", as is currently the case at OECD and EU level. This exercise should be aimed at developing effectively applicable rules that take account of data controllers' interests whilst ensuring a high level of protection for the rights at issue.
In this connection, one should also reconsider the conflict between the equivalence principle laid down in Chapter 3 of the Convention and the adequacy requirement set forth in Article 2 of the Additional Protocol. Most importantly, one should reconsider the concept and rules of transborder data flows in the light of new technologies (Internet, cloud computing) to specify what security measures should be taken if the use of such technologies entails cross-border data flows and/or the movement of data outside national borders. Additionally, it is fundamental to pay due attention to privacy principles when working out international rules concerning enforcement co-operation and access by law enforcement agencies to processing systems and data (in the individual jurisdictions) – which rules might possibly enhance those already set forth in CoE's Cybercrime Convention – as well as whenever such rules are developed in order to counter IT piracy and the latter may jeopardise data that are processed by any means which entails their processing outside national borders.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?
It is appropriate for the Convention to lay down unified rules that apply to both private and public entities. However, one might consider different mechanisms for implementing such unified principles to the individual sectors.

Role of the consultative committee
30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?
We believe the Consultative Committee's role should be strengthened also by developing its standard-setting, dispute resolution, and monitoring functions. However, the allocation of these tasks should be supported by provisions aimed at making available adequate human and financial resources.

Additional Remarks

It would also be appropriate to introduce specific wording on automated decisions, whereby an individual should be afforded the right not to be the subject of automated decisions that produce legal effects concerning him and/or impact significantly on him where such decisions are based exclusively on the automated processing of data intended to evaluate certain personal aspects related to him.

IURIDICUM REMEDIUM

1)Convention should be technologicaly neutral, but it is necessery to make special regulation for the use of some types of personal data (data retention...).

2)Definition of privacy and right to data protection should be opened (according to practice of the ECHR).

3) Definitions should be harmonized with other relevant regulations (for example in EU: directives 95/45/EC, 2002/58/EC, 2006/24/EC, EU decision on data transfer,...)

4) Data minimisation principle and the rule of proporcionality should be guiding principles of the Convention. Privacy by design is the essential approach in order to ensure data protection & privacy for the individuals worldwide, bureaucratic procedures should be minimized, if they are not useful for the data subjects needs but only for authorities.

5) Traffic and localisation data (digital communication) should be specialy protected. In EU (data retention directive) is the protection of this data insufficient. Data retention directive or national legislation was claimed unconstitutional by constitutional courts in Germany, Romania, Bulgaria or Cyprus. It is necessary regulate this problem in the documents of The Council of Europe.

6) It should be guaranted right to be not observed (RFID chips, confidentiality of information on internet etc.)

7) Class action or alternative dispute resolution mechanisms could be very effectual. The type of law suit is very similar **to consumer protection, where these solutions of disputes are successfully used.**

KAMPS DANIEL

Madame, Monsieur,
Vous demandez l'avis des Citoyens Européens concernant l'usage et le traitement des données à caractère privé et confidentiels.
Je vous remercie pour cette initiative, c'est bien la première fois que je suis directement consulté et concerné par l'élaboration d'une proposition de loi ou directive européenne !
Je suis l'auteur et le Webmaster du site Internet http://www.black-list.be (en cours d'édition).
Pour l'instant, 4 pages sont disponibles : Accueil – Assuralia – « Exemple à suivre » et Liens utiles.
La fédération des assureurs belges, par son « Groupement d'Intérêt Economique » GIE, Datassur est l'exemple extrême de toutes les dérives possibles permises dues au laxisme, au lobbying ou pire encore, par la corruption des fonctionnaires et mandataires politiques. Par manque d'initiative du législateur, des sociétés privées s'octroient le droit de combler les manquements les plus élémentaires des gestions par les collectes et les traitements des informations privées des Citoyens, provenant de différentes sources et parfois publiques, collectées par les Etats.

Voici donc mes propositions concernant les données informatisées et la protection de notre vie privée :

1. Déterminer et définir quelles sont les informations à caractère privé et personnel :
a) Concernant ma personne : nom, prénom, adresse, âge, sexe, état civil, nationalité, etc.
b) Les données du Registre National, Registre santé, Registre sécurité sociale (salaires, etc.) ;
c) Les données concernant la composition du ménage, propriétés (meubles, immeubles) ;
d) Les avoirs financiers et crédits ;
e) Toutes les données concernant nos véhicules (immatriculation, cylindrée, N° de chassis, N° du moteur, etc.).

2. Autoriser et promouvoir les bases de données publiques utilisées par les Etats membres pour utilité publiques ou pour la protection et les intérêts des Citoyens (en limitant fortement la diffusion) :
a) Le **Registre National** ;
b) La **Banque Nationale** (fichier de la centrale des crédits) pour éviter le surendettement ;
c) L'**ONSS** perçoit et gère les cotisations sociales patronales et personnelles par lesquelles il finance les différentes branches de la sécurité sociale (ONSS – en Belgique) ;
d) La **Banque carrefour de la sécurité sociale** est un organisme de droit public institué par la loi du 15 janvier 1990. Elle facilite l'échange électronique d'informations entre les acteurs de la sécurité sociale, tout en respectant les droits de chacun des bénéficiaires au respect de sa vie privée ;
d) Les informations des Parquets (condamnations judiciaires, etc.) ;
e) La DIV (Direction pour l'Immatriculation des véhicules).

3. Le droit à l'information : Permettre autant que possible d'accéder à toutes les informations par carte d'identité électronique ou autres (et promouvoir l'accès par les « Espaces Publics Numériques » – pour les citoyens ne possédant pas d'ordinateur ni de connexion à Internet). Les Etats membres utilisent les technologies informatiques très avancées – Le Citoyen a le droit aux mêmes technologies (accès par Internet) et dans la mesure du possible, ne pas devoir attendre plusieurs semaines pour obtenir les informations par voies postales.

4. Autoriser les sociétés commerciales, fédérations, associations à mémoriser les informations transmises par le Citoyen lui-même – Les documents papiers lus par les Citoyens sont généralement signés avec la mention « Lu et approuvé ». Trouver et utiliser une mention spécifique autorisant la mémorisation par procédé informatique et éventuellement le traitement de ces mêmes informations ;

5. Autoriser un accès très restreint aux informations privées récoltées et gérées par les Etats pour utilité publique et seulement dans l'intérêt et la protection du Citoyen ;

6. Ces mêmes sociétés doivent communiquer toutes les modifications concernant les traitements, compilation et modifications des données concernant le Citoyen dans les plus brefs délais ;

7. **Interdire impérativement la communication et l'échange des informations** reprises au point 4 entre différentes sociétés privées (cela peut faire effet de « boule de neige » et avoir pour conséquence de recevoir des publicités ciblées de multiples sociétés commerciales et de marketing, dans nos boîtes aux lettres, ainsi que dans nos boîte « E-mail – courriel). Exemple : lorsque une fédération quelconque désire utiliser les informations privées des Citoyens,

8. un formulaire spécifique complété par ce dernier devra accompagner l'inscription au club(de sport, de loisir, etc.) et interdire les cases à cocher avec mention en petits caractères ;

9. Déterminer précisément les personnes et services pouvant accéder à certaine informations déterminées pour des besoins spécifiques : policiers, juges, avocats, notaires (officier d'Etat), médecins, cliniques, hôpitaux, pouvoirs publics (écoles, communes, provinces, départements, etc.).

LITHUANIA / STATE DATA PROTECTION INSPECTORATE

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

As the Convention 108 has been drafted in a technologically neutral approach which is very important principle this principle stay as it is. A fundamental requirement of personal data protection is to respect for rights and fundamental freedoms, and in particular right of individual to privacy, with regard to automatic processing of personal data of every natural person in the territory of each Party of the Convention 108. There should be no constraints on the technical means by which data are processed, allowing any technologies on which data controllers are processing personal data but paying especial attention to measures dedicated to ensure execution of human rights and to data processing principles. As regards technologies they might be regulated by "soft" laws: recommendations, guidelines, opinions and etc.

2. Should Convention 108 give a definition of the **right to data protection** and **privacy**?

*Yes, definitions of the **right to data protection** and **right to privacy** might be given.*

The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12) as well as in the European Convention of Human Rights (Article 8) but no one of them do not provide the definition. The same approach is applicable to the definition of the right to data protection.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely **personal or household activity.** Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

It is arguable issue because the period between the Year 1980 and 2010 shows that personal data processing quickly and efficiently becoming more common, and on a larger scale. The dangers posed to safeguarding personal data (for example, through loss, destruction, accidental or malicious disclosure, or inaccuracy, especially misusing of data) may arise not only from legal entities, of professionals side, but it could be argued that the risk of those dangers from natural persons side had increased. Data collected of a purely personal activity might be lost or disclosed or misused in another ways.

5. The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The definition of the **controller of the file** should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?

Yes, there can be situations then for the file can be more than one data controller, so the definition of data controller may be reviewed.

6. New definitions may be necessary, such as for the **processor** or the **manufacturer of technical equipment**.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

The data minimisation principle is reasonable to add to the Convention as well as describe it more clearly in the explanatory memorandum.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Yes, it should be. Consent should be considered in close connection with the principle of an obligation to inform ("informed consent"). Present regulation use definition of "informed consent" only in health care and medical research spheres but it might be useful providing utilities, voting and etc. were data collection process is regulated by general principles and the legal basis like "entering to the contract", "ensure of public interest" and etc..

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Processing and use of personal data for purposes what are specified and legitimate and obligation not process them for purposes incompatible with the purposes determined before the personal data concerned are collected is one of the basic principles of data protection and national case law is based on it because of implemented Directive 95/46/EC so introducing this requirement will help to uniform a level of data protection in Parts of the Convention.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

The extended use and interest of special categories of data (health, sexual life and criminal convictions) as well as of biometric and genetic data and etc. from data controllers side requires special attention from the legislative point of view. The processing of these data might be regulated more precisely in the Convention. It might be reasonable to consider biometric and genetic data as special category of data.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific

provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

Children might be protected more than others groups of people in the context of use of communications technologies.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Yes, the notion of security may also include a right for data subjects to be informed of data security breaches.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Since the traffic and localisation data may revel a lot of information on persons' private life it may be considered to introduce special rules for the use of such data.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?
3
16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Rights – Obligations
17. The **right of access** should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the **logic** of the processing?

18. The **right of opposition** is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

20. Should a right 'not to be tracked' (RFID tags) be introduced?

Since the new technologies' use becomes more widespread it would be useful to introduce the right 'not to be tracked'.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

Yes, he (her) should have a right to remain anonymous when using information and communication technologies if these services or products are not personalized, for example internet, search engines and etc.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

Sanctions and Remedies
23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

No, class actions should not be regulated in the Convention very precisely because they are depending from national laws. The scope of alternative dispute resolution mechanisms might be regulated more clearly because it might be help for national supervisory authorities to collect common experience in ensuring of the rights of individual.

Data protection applicable law
24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Yes, it should be because there are many problems through jurisdictions implementing the laws on data protection on national level especially in data processing in communications field.

Data Protection Authorities
25. How to guarantee their independence and ensure an international cooperation between national authorities?

Some principles how the independence should be ensured also minimum requirements for international cooperation between national authorities should be introduced to the Convention.

26. Should their role and tasks be specified?

It might be, but not necessary.

Transborder data flows
27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

Role of the consultative committee
30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

Yes, it should be strengthened it the context of a possibility to ensure more harmonised approach in Parts of the Convention. Further cooperation of national authorities are also needed, as they have an important role in drafting of the laws and application of rules relating to the protection of personal data on national level. For this reason, the role of T-PD might be reviewed, with special attention to the cooperation between States-Parts of the Convention.

Useful links
[convention, add prot, modernisation, general website]

And You?
Please send us your reactions, thoughts, comments on any (or all!) of the points raised above, or any related issue which you consider important to address in the context of tomorrow's data protection.

MAURITIUS / ILE MAURICE - COMMISSARIAT A LA PROTECTION DES DONNEES

Objet et champ d'application de la Convention, Définitions

1. Rédigée selon une approche « technologiquement neutre », la Convention 108 est un instrument général et simple : peut-on conserver cette approche ou doit-on au contraire élaborer un texte plus détaillé ?

Un texte plus détaillé est requis.

*2. La Convention 108 devrait-elle définir le **droit à la protection des données** et le **droit au respect de la vie privée** ?*

Une définition large et générale de ces droits est importante.

3. La Convention 108 protège les individus contre toute atteinte portée à leur vie privée par des autorités privées et publiques, y compris la police et la justice. Cette approche globale doit-elle être conservée ?

Oui.

*4. La Convention 108 n'exclut pas de son champ d'application les données traitées par une personne physique pour l'exercice d'**activités exclusivement personnelles ou domestiques**. Doit-on maintenir cette approche, ou au contraire introduire une exception dans ce cas précis (dans le contexte spécifique du Web 2.0.) ?*

Il serait peut être important d'introduire une exception bien définie.

*5. La définition du **traitement automatisé** n'inclut pas la collecte des données : le fait que la collecte fasse l'objet d'une disposition spéciale est-il problématique ? Est-ce suffisant ? Doit-on ajouter d'autres opérations à la liste existante ?*

La liste d'opérations me semble restreinte et une définition large des opérations est requise pour englober toutes sortes d'opérations. La collecte devrait être incorporée dans la définition de traitement automatise pour éviter toute confusion quant au champ d'application de la définition.

*La définition du **maître de fichier** devrait être revue : plusieurs critères doivent-ils être répertoriés, ces critères doivent-ils se cumuler, peut-il y avoir plusieurs maître de fichier pour un seul fichier?*

Je propose une définition dans ses grandes lignes : « Le maître du fichier est toute personne physique ou morale, publique ou privée, qui décide de toute activité, automatisée ou non, entreprise sur les données personnelles". Plusieurs maitres de fichiers peuvent poser un problème d'ordre qualificatif en ce qui concerne l'application pratique de qui va tomber sous la définition et non.

*6. De nouvelles définitions sont peut-être nécessaires, comme celle du **sous-traitement** ou celle du **fabricant des équipements techniques**.*

Oui.

Principes de protection

*7. De nouveaux principes pourraient être ajoutés à la Convention, comme le principe de **proportionnalité** qui devrait s'appliquer à l'ensemble des opérations réalisées sur les données. Ce principe est également lié au **principe de minimalisation des données** qui vise à limiter la collecte des données à caractère personnel au strict minimum, voire à y mettre un terme quand cela est possible.*

Oui.

*8. La question du **consentement** devrait-elle être envisagée en étroite liaison avec le principe de transparence et l'obligation d'informer, ou en tant que condition nécessaire à satisfaire un traitement loyal et licite avant toute autre action ?*

Oui.

*9. La Convention 108 devrait-elle aborder la question de la **légitimation des traitements de données** comme le fait la Directive 95/46 dans son article 7 ?*

Oui.

*10. La Convention 108 ne fait pas de référence expresse à la **compatibilité nécessaire entre l'utilisation des données et le but** initial de leur collecte. Or, aujourd'hui, les données à caractère personnel sont généralement utilisées à des fins qui vont bien au-delà de celles initialement prévues, d'où la question de la compatibilité.*

Oui.

*11. La définition des **catégories particulières de données** faisant l'objet d'une protection accrue est très large, ce qui pourrait entraîner une application excessive de cette restriction : est-ce l'information ou son traitement qui est sensible ? Devrait-on ajouter d'autres catégories de données, comme les numéros d'identification (nationaux) et les données biologiques ou biométriques ?*

Il existe des données qui sont de nature sensible, ce qui relève non seulement du traitement mais de l'information elle-même et d'autres qui sont uniquement sensibles par rapport à leur traitement. Par exemple le nom d'une personne a caractère essentiellement non-sensible peut révéler l'origine raciale ou religieuse d'une personne de par son traitement mais une donnée biométrique peut être de nature sensible, ce qui requiert une distinction ou une catégorie séparée de ces données. Donc la distinction entre la nature et le traitement est peut-être requise.

*12. Une protection spécifique pourrait également être appliquée à certaines catégories de personnes sur lesquelles portent les données. Les **enfants,** en particulier, peuvent avoir besoin d'une protection spéciale en raison de leur vulnérabilité. Y-a-t-il un besoin de dispositions spécifiques à la protection des enfants ? Si tel est le cas, quels aspects devraient aborder ces dispositions ?*

Une protection spéciale est requise : les enfants doivent bénéficier d'un traitement ou les sites commerciaux sont obligés de dévoiler clairement leurs techniques de cueillette de

l'information et obtenir l'autorisation des parents avant de demander des renseignements personnels à des enfants de moins de 18 ans. Un fournisseur d'accès à Internet ainsi qu'un fournisseur de services de réseau devront aussi offrir un service de contrôle parental à leurs abonnés, limitant ainsi l'accès à un enfant, aux matières nocives et interdites par l'utilisation de leurs services; établir et maintenir des procédures et stratégies raisonnables pour protéger la confidentialité, sécurité et intégrité des données personnelles collectées sur les enfants.

*13. L'article 7 de la Convention porte sur la **sécurité** des données au sens restrictif du terme, à savoir la protection contre la destruction accidentelle ou non autorisée, la perte accidentelle et l'accès non autorisé, la modification ou la diffusion. La notion de sécurité devrait-elle également inclure un droit pour les personnes concernées d'être informées des violations de la sécurité des données ?*

Oui.

*14. Il existe certains risques découlant de l'utilisation des données de **trafic et de localisation** (données techniques accompagnant une communication) car ces données peuvent révéler les mouvements, orientations, préférences et associations avec d'autres. Avons-nous besoin de règles particulières pour l'utilisation de ce type de données ?*

Nous avons besoin premièrement de définir ces données dans la convention et les soumettre aux principes de protection de données personnelles sans qu'il y ait lieu de règles particulières sauf au cas contraire.

*15. Faut-il mettre en place des systèmes de **responsabilisation,** ainsi qu'une obligation de prouver que des mesures efficaces ont été prises pour garantir le plein respect de la protection des données ?*

Oui.

*16. Devrait-on appliquer le principe du « **respect de la vie privée dès la conception »** (Privacy by Design) qui vise à prendre en compte la question de la protection des données dès le stade de la **conception** d'un produit, d'un service ou d'un système d'information ?*

Oui.

Droits – Obligations

*17. Le **droit d'accès** ne devrait pas se limiter aux données mais devrait couvrir l'accès à l'origine des données, c'est-à-dire la personne qui est à l'origine de la communication. Ce droit devrait-il également couvrir l'accès à la **logique** du traitement ?*

Un droit d'accès devrait être aussi complet que possible, c.à.d, accès à toutes les procédures qui ont aboutit ou précèdent le traitement et qui sont nécessaires pour la connaissance de l'individu.

*18. Le **droit d'opposition** se justifie dans les cas où le traitement des données ne repose pas sur le consentement de la personne concernée. Le lien entre droit d'opposition et droit à l'oubli pourrait être examiné, ainsi que la possibilité de garantir le respect et l'exercice de ce droit.*

Oui.

19. Devrait-il y avoir un droit qui garantisse la confidentialité et l'intégrité des systèmes d'information ?

Oui, mais l'article 7 de la convention parle des mesures de sécurité appropriées, ce qui couvre aussi la confidentialité et l'intégrité.

20. Faudrait-il introduire le droit de tout individu à « ne pas être localisé / tracé» (identification RFID) ?

Oui, mais avec des exceptions raisonnables.

21. Les utilisateurs des technologies de l'information et de la communication devraient-ils avoir le droit de rester anonymes ?

Le principe d'anonymat est exclu des principes de protection de données personnelles. Tachons de savoir ce qui justifierait l'anonymat de ces utilisateurs.

22. La Convention 108 devrait-elle aborder la question du juste équilibre entre la protection des données à caractère personnel et la liberté d'expression (nouveau concept de la presse et du journalisme dans le contexte du Web 2.0.) ?

Oui.

Sanctions et recours

23. Devrait-on introduire des recours collectifs dans la Convention ? Faut-il examiner l'introduction d'autres mécanismes de règlement des litiges ?

Oui.

Droit applicable en matière de protection des données

24. Doit-on envisager une règle qui déterminerait le droit applicable au traitement des données (dans les cas où différentes juridictions sont concernées) ?

Oui.

Autorités de protection des données

25. Comment garantir leur indépendance et assurer une coopération internationale entre les autorités nationales ?

La coopération doit se faire d'une façon générale respectant la souveraineté et les lois du pays.

26. Faut-il spécifier leur rôle et leurs missions ?

Oui.

Flux transfrontières de données

27. La Convention 108 avait pour but de concilier la protection effective des données et la libre circulation de l'information sans considération de frontières. Ces principes ont été développés plus

avant dans un protocole additionnel (STCE 181, 2001). En principe, un niveau de protection adéquat doit être assuré.

Oui.

28. Doit-on entièrement réexaminer la notion de « flux transfrontières de données » à l'heure d'Internet, où les données circulent instantanément à travers les frontières ? Serait-il utile de fixer des règles minimales internationalement reconnues pour garantir le respect de la vie privée sans considération des frontières ? Quel pourrait en être le contenu ?

Oui, on peut commencer par déterminer la loi applicable et des critères tel que les données ne doivent pas être transférées a l'insu de l'individu sans son consentement sauf cas contraire tel que les besoins judiciaires, intérêt public ou national, l'exécution d'un contrat etc. ; ou dans le cas que le pays destinataire n'offre pas de protection adéquate.

29. Doit-il y avoir des règles différentes pour le secteur public et le secteur privé ?

Les principes resteront les mêmes. Il faut peut-être identifier certaines règles inapplicables à l'un ou l'autre des secteurs.

S'agissant notamment du secteur privé, doit-on avoir davantage recours à des règles d'entreprise contraignantes, éventuellement associées à un système de responsabilisation du destinataire final pour garantir le respect de ces règles ?

Oui.

Rôle du comité consultatif

30. La Convention 108 a créé un comité chargé de faciliter son application et, le cas échéant, de l'améliorer. Doit-on renforcer le rôle jusqu'ici principalement consultatif du comité ? Si oui, quelles fonctions faut-il développer plus avant : l'activité normative, le règlement des litiges, le suivi ?

Une autorité contraignante en matière de protection de données personnelles à laquelle les autorités nationales y compris les individus peuvent avoir recours est importante.

MORPHO – GROUPE SAFRAN

Paris, le 10 mars 2011

REPONSE DE MORPHO – GROUPE SAFRAN

à la consultation du Conseil de l'Europe sur la modernisation de la convention 108

Morpho (groupe Safran) est une société de haute technologie, acteur majeur de l'identification, de la détection et des documents électroniques dans le monde. Morpho est spécialisée dans les applications de gestion des droits des personnes ou de flux utilisant notamment la biométrie (n°1 mondial), les terminaux sécurisés et la carte à puce. Ses équipements et systèmes intégrés contribuent, dans le monde entier, à la sûreté des transports, à la sécurisation des données, à la sécurité du citoyen et au maintien au plus haut niveau de la sûreté des États.

A l'occasion du 30ème anniversaire de sa Convention 108 sur la protection des données, le Conseil de l'Europe a lancé une consultation publique interrogeant sur la nécessité de moderniser le texte à la lumière des nouveaux défis liés à la fois aux évolutions technologiques et à la mondialisation. Morpho souhaite apporter sa contribution à cette initiative, sans pour autant répondre à l'ensemble des questions posées par la consultation.

Question 7 : de nouveaux principes pourraient être ajoutés à la Convention, comme le principe de proportionnalité qui devrait s'appliquer à l'ensemble des opérations réalisées sur les données. Ce principe est également lié au principe de minimalisation des données qui vise à limiter la collecte des données à caractère personnel au strict minimum, voire à y mettre un terme quand cela est possible.

Le principe de proportionnalité est l'un des principes clefs qui gouverne aujourd'hui la directive européenne 95/46. Ce principe qui vise à assurer un équilibre entre le traitement des données et la finalité poursuivie, en dépit de ses vertus intrinsèques, n'a pas permis de satisfaire aux besoins de visibilité et de sécurité juridique des opérateurs économiques. En effet, il repose sur une démarche éminemment subjective qui donne lieu à des interprétations très différentes en fonction de l'autorité de protection des données qui l'apprécie, il se traduit dès lors par des solutions très divergentes, ce qui ne favorise pas une distribution industrielle adressant différents pays. Ainsi, lorsqu'elles examinent un même dispositif biométrique installé dans des circonstances similaires et dans un environnement similaire, à la lumière du principe de proportionnalité, les autorités de protection des données apportent des réponses contradictoires. C'est la raison pour laquelle, il nous apparait souhaitable que, ce principe, s'il était retenu et consacré par le texte révisant la Convention 108, soit accompagné par des dispositions de nature objective. A titre d'exemple, la Convention révisée pourrait encourager le recours à des procédures de labellisation/certification reposant sur des critères précis, que l'industriel devrait respecter pour déployer ses produits. Elle pourrait également encourager une approche par la co-régulation visant à inciter les différentes parties prenantes (décideurs politiques et industriels) à définir conjointement des critères à respecter dans un secteur donné.

Question 11 : la définition des catégories particulières de données faisant l'objet d'une protection accrue est très large, ce qui pourrait entrainer une application excessive de cette restriction : est-ce l'information ou son traitement qui est sensible ? Devrait-on rajouter d'autres catégories de données, comme les numéros d'identification (nationaux) et les données biologiques ou biométriques ?

Le Conseil de l'Europe s'interroge sur la pertinence de réviser la définition des « catégories particulières de données » couvertes par la définition actuelle de l'article 6 de la Convention 108, à savoir les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, les données à caractère personnel relatives à la santé ou à la vie sexuelle ou les données à caractère personnel concernant les condamnations pénales. Ces données ne peuvent par principe faire l'objet d'un traitement automatique à moins que le droit interne ne prévoie des garanties appropriées. Ainsi, ces « catégories de données particulières » pourraient elles être étendues pour couvrir les données biométriques. Morpho souhaite à cet égard rappeler un certain nombre d'éléments qui montrent qu'il ne serait pas justifié de soumettre les données biométriques au même régime juridique que les données aujourd'hui visées par l'article 6.

L'empreinte digitale révèle bien moins d'informations que le nom d'un individu

Elle ne permet pas de déterminer l'origine, l'appartenance religieuse réelle ou supposée ou l'état de santé d'une personne. Comme nous l'avions déjà souligné, s'il est vrai que certains facteurs tel que le vieillissement, certaines professions, certains traitements thérapeutiques, ou certaines maladies (dysplasie) sont susceptibles d'altérer les empreintes digitales, à l'inverse, le fait qu'une empreinte soit altérée ne permet pas de préjuger de la cause de la dégradation. De surcroît, Il est plus facile d'obtenir des informations sur un individu à partir de son nom que de son empreinte digitale. Contrairement au nom, elle ne donne aucune indication sur l'origine ethnique ou sur l'appartenance à une religion réelle ou supposée. Avec un nom, il est aisé de collecter de nombreux renseignements sur un individu sans expertise technique particulière : il suffit d'effectuer une recherche sur internet. Dès lors que les données biométriques fournissent moins d'information sur un individu que son nom pourquoi les soumettre à un régime juridique plus contraignant ?

La reconnaissance faciale : le visage est une information publique

S'il est incontestable qu'une photo de visage est susceptible de révéler des informations sur l'origine raciale ou ethnique, le visage est tout comme le nom une information publique qui saurait difficilement être qualifiée de donnée sensible. Force est de constater que dans la pratique, les photographies de visage susceptibles de faire l'objet d'un traitement automatique sont extrêmement répandues, en raison de l'adoption massive des appareils photos numériques et du succès des réseaux sociaux. Dans le même temps, de nouvelles fonctionnalités se développent sur les sites de partage de photos tels que Picasa (Google), i-Photo (Apple) ou FlickR (Yahoo) qui facilitent l'indexation et le partage des photos. Ces applications permettent de scanner automatiquement les photos, de détecter, reconnaitre les visages et de les tagger. Après avoir lancé une application de détection des visages afin de classer facilement les personnes qui apparaissent, Facebook a récemment annoncé une nouvelle application de reconnaissance faciale afin d'automatiser le processus de *tagging* dans les albums, l'application suggèrera le nom des individus qu'elle aura reconnus. Se constituent ainsi des bases de données biométriques à grande échelle qui échappent

aux règles relatives à la protection des données. Doit-on dès lors considérer que l'ensemble des photos mises en ligne sont des données sensibles ? Quels recours pourraient être exercés alors même que les serveurs des sites visés se trouvent le plus souvent en dehors de la juridiction des Etats membres de l'Union Européenne ? Comment le droit peut-il appréhender ces bases de données biométriques à grande échelle ? Serait-il légitime et proportionné de leur accorder un régime dérogatoire alors que des bases de données biométriques plus restreintes feraient l'objet de procédures et de contrôles beaucoup plus sévères ? Dans un environnement fortement concurrentiel, tel que la biométrie, serait-il justifié de favoriser les entreprises basées hors de l'Union Européenne ?

La reconnaissance vocale :

Les opérateurs de communications électroniques (fixe, mobile, FAI) proposent aujourd'hui à leurs utilisateurs des systèmes de messagerie vocale, intégrant des fonctionnalités permettant d'identifier le nom ou le numéro de l'appelant, ainsi que la date et l'heure de l'appel. Les messages déposés sont stockés, non pas en local sur le terminal de l'utilisateur, mais sur des serveurs gérés par l'opérateur constituant d'importantes bases de données biométriques. En outre, les systèmes de messagerie unifiée permettent de convertir les messages vocaux en fichiers numériques contenant l'empreinte vocale du correspondant qui peut dès lors être transférée, archivée ou convertie en fichier texte. La facilité avec laquelle peuvent être constituées des bases de données vocales à l'insu des personnes doit-elle pour autant conduire à qualifier les empreintes vocales de données sensibles ? Doivent-elles bénéficier d'un régime juridique différent des empreintes digitales et sur quel fondement ?

Les empreintes génétiques :

Il convient de distinguer les données génétiques au sens médical du terme, des « empreintes génétiques » utilisées à des fins d'identification. Les premières permettent d'obtenir des informations sensibles indiquant des prédispositions d'une personne à certaines maladies, elles peuvent également permettre de déterminer l'origine raciale ou ethnique au sens de l'article 8 de la directive 95/46/CE, elles sont donc des données sensibles. En revanche, en matière de police scientifique, l'empreinte génétique utilisée à des fins d'identification, ne permet pas de révéler précisément certaines des données sensibles du patrimoine génétique de la personne, que ce soit de manière partielle ou complète. En effet, les marqueurs utilisés sont ceux de la zone non codante de l'ADN (i.e qui ne donne aucune indication sur la santé, ou sur les prédispositions à certaines maladies). S'agissant de l'origine ethnique ou raciale, des études statistiques menées à la demande de gouvernements ont permis de montrer que la fréquence de certains allèles (données) chiffrées qui caractérisent les marqueurs) donne des indications sur la probabilité statistique d'appartenance à une origine, mais le raisonnement ne s'effectue que sur un seul marqueur, le risque d'erreur est donc élevé.

Non seulement la biométrie n'est pas une donnée sensible mais elle peut permettre d'assurer l'anonymat

Dans certaines situations, l'utilisation de données biométriques (empreinte digitale ou iris) peut permettre de protéger la vie privée des individus concernées. Les données biométriques anonymisées permettent de déterminer si un individu peut se voir ou non accordé un droit sans que son identité ne soit dévoilée. Ainsi, certains établissements hospitaliers aux Etats-Unis recourent à la

biométrie pour gérer les dossiers médicaux des personnes sans domicile fixe, dans le respect de l'anonymat. En Australie, les doses de méthadone sont distribuées, non pas sur présentation d'un titre de santé ou d'un titre d'identité mais par le recours à la biométrie. Le système « Methadose » scanne l'iris des patients qui ainsi identifiés se voient distribuer de façon automatique la dose de méthadone prescrite, ce qui non seulement permet d'éviter les risques erreurs liés à des homonymies, mais également d'empêcher les trafics associés à la distribution de substance pouvant agir comme drogue de substitution.

<u>Question 13</u> : l'article 7 de la Convention porte sur la sécurité des données au sens restrictif du terme, à savoir la protection contre la destruction accidentelle ou non autorisée, la perte accidentelle et l'accès non autorisé, la modification ou la diffusion. La notion de sécurité devrait-elle également inclure un droit pour les personnes concernées d'être informées des violations de la sécurité des données ?

Le Conseil de l'Europe envisage d'introduire un droit d'être informé des violations de sécurité pour les individus concernés. Ce droit à l'information des violations de sécurité s'il nous apparait utile, devrait néanmoins être expressément justifié par la nécessité de protéger l'identité et de limiter les risques d'usurpation d'identité. En effet, le droit à l'identité et à sa protection doit être au cœur des règles qui encadrent la protection des données. Sans intégrité de l'identité, les autres données personnelles ne peuvent être sauvegardées. La modernisation du texte devrait être l'occasion de prendre pleinement la mesure des enjeux que représente l'identité tant dans le monde physique que numérique, et de son importance au regard de la protection des autres données personnelles.

<u>Question 16</u> : Devrait-on appliquer le principe du « respect de la vie privée dès la conception » (Privacy by Design) qui vise à prendre en compte la question ou la protection des données dès le stade de la conception d'un produit, d'un service ou d'un système d'information ?

Le principe de « Privacy by Design » est aujourd'hui un principe proclamé dans de nombreuses enceintes. Il a fait l'objet d'une résolution adopté par la 32eme conférence internationale des autorités de protection des données en octobre 2010. La Commission Européenne souhaite également le prendre en considération dans le cadre de la révision de la directive 95/46. Dans cette perspective, il nous semble cohérent que ce principe soit également consacré par la Convention du Conseil de l'Europe.

Néanmoins, si Morpho se félicite de la reconnaissance de ce principe, elle considère que sa simple consécration n'est pas suffisante. Pour être opérationnel, ce principe doit pouvoir être décliné en critères concrets suffisamment précis pour garantir la sécurité juridique. L'élaboration de ces critères ne relève bien évidemment pas de la compétence du Conseil de l'Europe, toutefois il nous apparait qu'il pourrait être souhaitable que le Conseil de l'Europe encourage le recours à des mécanismes de labellisation ou à la certification. Cette approche complémentaire aux actions du Conseil de l'Europe permettrait de construire une liste de critères connus par les industriels, spécifiques à un secteur d'activité et évalués par une autorité de labellisation indépendante. Elle permettrait d'assurer une visibilité à long terme pour les opérateurs économiques tout en apportant la confiance nécessaire aux utilisateurs. Le concept de Privacy by Design doit se traduire dans sa mise en œuvre par des solutions économiquement et techniquement viables.

SAFRAN
Morpho

En outre, le risque associé au traitement de la donnée personnelle doit être évalué. Une approche basée sur le risque permettrait, en effet, d'apporter des garanties nécessaires à la protection des données : garanties de qualité pour les clients, pour les assureurs du point de vue de la sécurité, tout en garantissant que les données personnelles ne puissent être détournées.
Cette approche implique de développer une méthodologie reposant sur l'évaluation du risque : identification du périmètre du risque, évaluation des niveaux de risques et des vulnérabilités, élaboration de scénarios, évaluation de la probabilité de réalisation et du niveau d'impact, évaluation des mesures de contrôles, mais aussi de développer et mettre en place des outils adaptés, tant du point de vue technique qu'économique, en réponse aux risques identifiés.

En conclusion, Morpho considère que :

- il ne serait pas justifié d'étendre la portée de la définition des données sensibles aux données biométriques ;
- le concept de « Privacy by Design » doit être décliné en critères concrets et précis et assurer suffisamment de visibilité aux industriels. Si l'approche auto-régulation nous parait insuffisante car permettant trop de flexibilité, d'autres voies (labellisation, certification, «meilleures techniques disponibles) doivent être explorées plus avant. En tout état de cause il serait souhaitable que le risque associé au traitement soit évalué ;
- le droit à l'identité et à sa protection doit être affirmé. Ce droit est au cœur de la protection des données. Cette assertion doit être le pendant de l'obligation de notifier les violations des données

MYDEX

Response from Mydex Community Interest Company

Introduction

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

The current approach is not sustainable.

2. Should Convention 108 give a definition of the right to data protection and privacy?

Yes

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes, with more emphasis put on transparency of law enforcement activities at the macro level.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

This is an area that demands further analysis and discussion. Mydex (and many others, including the World Economic Forum) believe that next generation technical architectures will place the individual at the centre of their own personal data eco-system, in effect acting in the role of Data Controller. Laws will need to reflect and enable this new modus operandi (this data empowerment by design, a side benefit of which is much improved privacy and data protection).

This is a 'here and now' issue, not some futuristic scenario; Mydex have recently completed a pilot exercise in which 3 UK local authorities 'subscribe to' and individual and their personal data store. Planned live service is late 2011.

Mydex Data Services CIC, All rights reserved

Response from Mydex Community Interest Company

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?

As per above, their absolutely needs to be more flexibility in definitions, and specifically enable the multiple controller scenario.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Yes, also note the emergence of 'agents' (including automated ones) acting on behalf of the individual; taking on power of attorney where necessary and appropriate.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Yes, as per above, if the individual is placed at the centre of the eco-system, many benefits arise - economic benefits will be huge, and data minimisation/ non-collection will be the norm.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Consent must become a more active and meaningful component.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

Mydex Data Services CIC, All rights reserved

Response from Mydex Community Interest Company

Yes

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Yes, compatibility would be a valuable addition.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

Yes, lack of detail in current legislation allows most of the current work-arounds.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

Not sure these can be made workable in law.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Yes

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data ?

Yes

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Mydex Data Services CIC, All rights reserved Document Manager: Name

Response from Mydex Community Interest Company

Yes

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Yes, and built on; data empowerment is the real end game with privacy a valid half-way stage.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

Yes

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

Yes

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

Yes

20. Should a right 'not to be tracked' (RFID tags) be introduced?

Yes

21. Should everyone have a right to remain anonymous when using information and communication technologies?

Yes

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and

Mydex Data Services CIC, All rights reserved

journalism in the context of Web 2.0.)?

No

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

Yes, class actions would be valid option.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Absolutely, cloud computing necessitates this.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

Probably not do-able.

26. Should their role and tasks be specified?

Yes

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

Mydex Data Services CIC, All rights reserved

Response from Mydex Community Interest Company

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

Yes

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules.

The bar should be set equally for both.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

No

And You?

Please send us your reactions, thoughts, comments on any (or all!) of the points raised above, or any related issue which you consider important to address in the context of tomorrow's data protection.

Email us before 10 March at: data.protection@coe.int!

Mydex Data Services CIC, All rights reserved

POCS MATTHIAS

Data Protection in the Police Sector

Matthias Pocs, LL.M. (matthias.pocs@uni-kassel.de)

Interferences with fundamental rights to privacy and data protection in the police sector should be given special attention in tomorrow's data protection. In particular, the police will use detection techniques like biometric systems in future. Therefore, challenges to the law will occur. For example, it will have to be decided upon how to proceed when suspects and nonsuspects are confused due to error rates of biometric systems. In order to avoid contradictory European and national provisions, I would like to urge all stakeholders to consider high-level harmonization of these substantive matters and inter-institutional cooperation between CoE and EU.[1]

This document contains recommendations for regulation that have already been discussed (see 1.-3. and 5.) as well as factual challenges that have been recognized but have not been given legal standing yet (see 4., 6. and 7.).

[1] Concerning COM(2010) 609 final, the timing is perfect.

Summary

Convention 108 should provide:

- that processing of personal data for purposes other than those specified be permitted of if the data subject is suspected of a grave form of crime and adequate safeguards against violations of human dignity are laid down.[2]
- that designers, producers and controllers ensure that filing systems are designed in a way that the categories of personal data that are necessary to distinguish between the data subjects in accordance with the purposes for which they are processed, can be stored.
- that the award of procurement contracts take into account that specific risks to the fundamental rights of data subjects are avoided or minimized by technology design.
- for the same protection regime for data collection as for further processing.
- that, subject to the other Articles in Convention 108, the designers, producers and controllers ensure that the filing system used for detection of crimes and suspects is designed in a way that the controller is able, on the request of the supervisory authority, to demonstrate, in an aggregated format, how many data sets have been processed and how.
- that, if a filing system is used for detection of crimes and suspects which are subject to significant error rates,
  a) the results from operational tests of that system must be notified prior to its deployment,
  b) only an independent authority can alter the decision policy.
- that from the best available techniques in the meaning of Directive 96/61/EC, controllers should choose the technology that minimizes the risk of false automated decisions that are more likely to affect a certain ethnic category of data subjects.

[2] The following recommendations are in boldface type in the body of this document.

1 Scope

Question 3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Convention 108 is an important legal instrument in the context of law enforcement and crime prevention ("the police sector"). Since the Data Protection Directive 95/46/EC is not applicable (also Art. 3 (2)), EU data protection instruments in the police sector rely on the Council of Europe Convention ETS no. 108.[3] Unfortunately, some countries have not ratified the protocol ETS no. 181 which requires the establishment of an independent data protection authority.

For specification of the Convention ETS no. 180, the Recommendation R (87) 15 which sets out the principles of Convention 108 for the police sector, is often referred to.[4] This shows that the comprehensive approach of Convention 108 is important.

Violations of fundamental rights protected by the CoE Human Rights Convention are more likely the more grave the interference with those rights is. This view is in line with the approach chosen for assessing gravity of interferences under the Human Rights Convention. The ECtHR holds that there is a "margin of appreciation" that is left to the competent national authorities in this assessment. The breadth of the margin of appreciation depends on, among other factors, the nature of the interference and the object pursued by the interference.[5] In particular, Member States may introduce special investigation techniques used for detecting crimes and suspects,[6] such as biometric systems for crowd scanning. Detection of suspects means that data about nonsuspects need to be processed in order to find out whether or not the data subject is a suspect. Nonsuspects do not give the police reason for processing personal data and interference is therefore particularly grave.[7] In the light of the "margin of appreciation" doctrine, the regulation of such interference should in any case remain within the framework of Convention 108.

2 Purpose limitation and secondary use

Question 10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

An exception to the purpose limitation principle is unacceptable because purpose specification and limitation are core data protection principles and give substance to the fundamental requirements of foreseeability and nonarbitrariness as provided for in the European Convention of Human Rights, in particular, for the police sector.[8] In Germany, for example, the Federal Constitutional Court holds that the purpose of data processing in the police sector must be specified as an actual danger (as

[3] E.g., in Art. 8 Framework Decision 2006/960/JHA („Swedish Initiative").
[4] E.g., in Art. 8 Framework Decision 2006/960/JHA („Swedish Initiative").
[5] See for example, *S and Marper v. UK*, nos. 30562/04 and 30566/04, para. 102 w. f. r.
[6] Recommendation 2005 (10).
[7] See e.g., in Germany, BVerfGE (collection of BVerfG decisions at: http://www.servat.unibe.ch/dfr/) 120, 378 (402); 115, 320 (354); 113, 348 (383); 113, 29 (53); 109, 279 (353); 107, 299 (320f.); 100, 313 (376, 392).
[8] Lately for example, *Uzun v. Germany*, no. 35623/05, 20ff. w. f. r.

opposed to potential dangers).[9] Specifying the purposes of data processing in the police sector is particularly important since the general requirements in police law are often too vague.[10]

The Convention 108 should provide for a consistent regulation within the data protection framework. For the police sector, the purpose specification principle should take into account the specificities. Although purpose specification is a core principle of privacy and data protection, suspicion of a crime may justify limitation to the suspect's privacy and data protection.[11]

Such limitations of suspects' rights could comprise the secondary use of data relating to suspects. It could explicitly be provided that for grave forms of crime secondary use of personal data is allowed. This explicit limitation for grave forms of crime would also strengthen the rights of data subjects that are suspected of less or moderately grave forms of crime. If a crime is particularly serious,[12] data about the criminal can be subject to a relaxed purpose limitation because secondary use is more likely to be justified. Secondary use could be deemed compatible with the original purposes. This flexible concept of compatibility enables the legislator to take into the specificities of the police sector within the legal framework, rather than resorting to derogations and exemptions. Such high-level harmonization would guarantee protection against both threats to public security and risks of data processing.

Consequently, **Convention 108 should provide that processing of personal data for purposes other than those specified** is prohibited if the data subject is suspected of a less or moderately grave form of crime and **permitted of if the data subject is suspected of a grave form of crime and adequate safeguards against violations of human dignity[13] are laid down.**

3 Distinction between data subjects

Question 6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Question 16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

The principle of privacy by design should be introduced. This principle does not only address the controller but also the designer and manufacturer (producer) of filing systems. The example of distinction between data subjects in relation to police detection techniques illustrates the need for regulating this principle.

Effectiveness of the purpose limitation principle is at risk if there is no requirement to distinguish data in accordance with their degree of accuracy and reliability, that data based on facts should be

[9] BVerfGE 120, 378 (428); 115, 320 (346); 113, 348 (377f., 387ff.); 109, 279 (350ff.); 100, 313 (383f.).
[10] See e.g., S. 21 (1) Federal Police Act: The Federal Police may, save where otherwise provided, collect personal data so far as this is necessary to fulfil the tasks incumbent on them.
[11] See also European Commission, COM(2010) 609 final, p. 14.
[12] "Serious" according to the general principles and the common values enshrined in the Convention and the Charter.
[13] Human dignity could be violated, for example, if an information system contains full text fields which allow entering any kind of data (Stubenrauch, Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten, Nomos 2009).

distinguished from data based on opinions or personal assessments, and between different categories of data subjects (criminals, suspects, victims, witnesses, etc.) and other nonsuspects.[14]

The risks for the nonsuspects are significantly increased if data about a large number of citizens are captured by automatic means and compared with data about nonsuspects. On one hand, the increase of risks relates to the capture of data relating to them, to which also persons that are entirely uninvolved are subject, on the other, to the use of references in databases relating to them.

Data subjects may be discriminated against because they are not treated like uninvolved persons but like potential criminals and may be subject to automated decisions (see 4.) and possible further measures. This discrimination may in particular be detrimental if the purpose of the system deployment is changed afterwards.

For example, in case of car number plate recognition, after system deployment other purposes were pursued (2007 in Hesse: 67 % Breaches of car insurance law) than originally planned (Combatting cross-border crime, prevention of offences like burglary and support of search for lost property).[15]

In order to distinguish between data subjects, the deployed system has to be designed in a way that the necessary data may be put in and stored. If data fields are missing, it is impossible to store the necessary categories of information (e.g., being a witness or a contact person). In addition, distinction may have to be made between less, moderately and grave forms of crime. Without having made such distinction, the personal data are incomplete and therefore inaccurate because from a technical point of view, nonsuspects are equated with suspects. This violates the principle of data accuracy according to Art. 5 (d) Convention 108.[16]

Unjustified interferences could be avoided by providing that **designers, producers and controllers ensure that filing systems are designed in a way that the categories of personal data that are necessary to distinguish between the data subjects in accordance with the purposes for which they are processed, can be stored.**

Such a distinction between data subjects would consistently combine the principles of data accuracy and privacy by design. To this end, for the data sets in the reference database, specific data fields would have to be defined. Within the system, it could then be determined what values the data fields may store in order to decide whether or not a data set should be used (e.g., for the automated decision of suspicion). By defining the data fields and system policy, the distinction between data subjects in accordance with the purposes is possible.

4 Error rates

The introduction of the *privacy by design principle* is important in detection systems, in particular, those for biometric recognition. These systems entail issues of data accuracy and fairness due to the pattern recognition technology. Such issues can only be resolved by the designers and producers of the technology. Hence, the example of the error rates shows the need for the introduction of the principle of privacy by design.

[14] European Commission, COM(2010) 609 final, p. 13; for Germany, Pocs, DuD (Datenschutz und Datensicherheit) 2011, p. 163.
[15] Bodenbenner, NVwZ (Neue Zeitschrift für Verwaltungsrecht) 2010, 679.
[16] Also Art. 6 (1) (d) DPD, Para. 8 OECD Guidelines 1980 and Paras. 1 and 2 UN Guidelines 1990.

In particular, biometric systems such as face and fingerprint recognition within countries and at the border (airports, railway stations etc.) will serve to find known suspects in a crowd of people.[17] The specific feature of these systems is that non-digital characteristics are captured by automatic means and further processed. Such processing **is subject to significant error rates**.[18] Lately, for example, the European Data Protection Supervisor pointed to the risk "related to inherent inaccuracies in the collection and comparison of biometric data."[19]

In biometric systems, the characteristics may be falsely captured and attributed. This may be due to lighting conditions; unsuitable characteristics; impostors; errors of measuring, operating and processing; system policies; or similarities between two data subjects. Consequently, suspects may not be recognized (**false non-matches**) and citizens may falsely be suspected (**false match**). The false result of the comparison may also refer to a candidate list, that is, a list of several potential suspects. Hence, if biometric characteristics are wrongly captured or falsely matched with a suspect's identifier, persons can be confused with suspects.

Further, the risk of confusion may be higher for some ethnic groups because persons are similar to the known suspects (see below).

The risk of confusion is not new, since with manual checks, too, personal characteristics can be wrongly associated with those of suspects'.[20] However, due to automation, the number of data captures multiplies. This multiplication causes a novel risk of confusion if a large number of citizens are subject to the data processing. Therefore, protection against the societal risks of error rates is needed.

In order to weigh up the error rate against the purpose of the deployed biometric system, the extent of the risk has to be ascertained. For biometric systems, this extent can only be ascertained if the deployment is tested:

> *There is a general lack of publicly available scenario and operational evaluations of FRT [facial recognition technology]. This means that policymakers and users often need to depend on technology evaluations […] (which cannot be extrapolated to operational implementations) and the information provided by vendors (which are obviously not independent and are always the results of very small tests). Recommendations: Publicly funded scenario and operational evaluations are needed to support policy makers in making decisions about the appropriate use of FRT.*[21]

---

[17] a) German Federal Criminal Office, operational test of Facial recognition system at a railway station, Final Report (English), http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_final_report.pdf; and b) 3-D facial recognition systems researched in the European FP7 project "3dface," see Busch/Nouak, DuD (Datenschutz und Datensicherheit) 2008, 126.
c) securing of fingerprints on luggage at airports researched in a project funded by the German Federal Ministry of Education and Research): Hildebrandt/Ulrich/Pocs/Dittmann, BioID 2011 (to be published).

[18] For verification systems, this is known by legislators for some time already, e.g., German Parliament, Drucks. 14/8839, 22.04.2002. Detection systems suffer from significantly larger error rates.

[19] EDPS, Opinion of 30.09.2010, para. 45.

[20] BVerfG RDV 2005, 214: Due to the technical procedure of drug screenings it was possible to accurately determine remains of drugs in persons doing military service but not to accurately attribute the test results.

[21] Nissenbaum/Introna, Facial Recognition, New York 2010, S. 38.

Such an operational test is, e.g., the test of the Federal Criminal Office of Germany.[22] Further, the following aspects for risk assessment are often ignored:

> *(1) large populations (the biometric double problem), (2) a significant age difference between gallery and probe image (the time delay or freshness/staleness problem) and (3) relatively uncontrolled environments (illumination, rotation, and background). […] There seems to be no publically available evaluation of falsification strategies.*[23]

Convention 108 should **provide that, if a filing system is used for automated decisions of suspicion which are subject to significant error rates, the results from operational tests of that system**, which take these aspects into account, **must be notified prior to its deployment. Only an independent authority** (data protection authority or judge) should be able to **alter the decision policy** (such as the threshold of degree of similarity between a biometric probe and a reference)**.**

The legal consequence that is tied onto the assessment of the error rate and a violation of the principle of data accuracy[24] could be disproportionality of the system deployment. Proportionality could be established by procedural precautions, which guarantee that data subjects are treated like nonsuspects, or technology design, which reduces the error rates or minimizes data processing.

Finally, certain ethnic groups of data subjects are often over-represented in biometric reference databases.[25] In order to avoid violation of the fairness principle[26] which prohibits discriminating against data subjects,[27] **from the best available techniques in the meaning of Directive 96/61/EC,**[28] **controllers should choose the technology which minimizes the risk of false automated decisions of suspicion that are more likely to affect a certain ethnic category of data subjects.**

5 Procurement law

The introduction of the *privacy by design principle* may be enforced by using the mechanisms of public procurement. Processing of personal data in the police sector relies on technology designers and producers which may be involved in formal procurement procedures. The connection with public procurement law offers the opportunity to create competition for technology design that optimizes protection of the fundamental rights to privacy and data protection. Connecting the future Directive with procurement law would thereby promote the materializing of the principle of privacy by design. Interference with the fundamental rights to privacy and data protection should be taken into account when awarding public contracts to technology producers.

This requirement should be proportionate to other criteria of the procurement procedure and therefore only comprise interferences entailing specific risks such as processing data relating to a large number of nonsuspects (Part II). Hence, Convention **should provide that the award of**

---

[22] Federal Criminal Office of Germany, see above.
[23] Nissenbaum/Introna, see above.
[24] Data accuracy, up-to-dateness, and completeness, Art. 5 (d) ETS no. 108; Art. 6 (1) (d) DPD; also para. 8 OECD Guidelines 1980, paras. 1 and 2 UN Guidelines 1990 and para. 21 APEC Privacy Framework.
[25] See for example, ECtHR, *S and Marper v. UK*, nos. 30562/04 and 30566/04, para. 124.
[26] According to Art. 6 (1) (a) DPD and Art. 5 (a) Convention ETS no. 108.
[27] This specification has been made explicit in Article 6 (2) of The Madrid Standards, 5 November 2009, at: http://www.privacyconference2010.org/upload/2009-1.pdf
[28] See http://www.edps.europa.eu, "B" of the data protection glossary.

procurement contracts take into account that specific risks to the fundamental rights of data subjects are avoided or minimized by technology design.

6 Data collection for detection techniques

Question 5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The protection regime governing *data collection* could be too weak if it is not aligned with the further phases of data processing. This may be illustrated using the example of detection techniques. The gravity of interference resulting from collecting and processing data relating to nonsuspects by automatic means may be little from an individual's point of view. Such an automated decision in case of a nonsuspect processes data for a short time and they are deleted without further use. However, the entirety of interferences with the rights of nonsuspects may justify the need for protection of the society from specific risks.

In Germany, for example, the fundamental rights to privacy and data protection do not only serve to protect individuals but also the "public good because [privacy and data protection] are an elementary condition to a free democratic community that is based on the ability of its citizens to act and cooperate."[29] For the police sector, it was held that the fact that a large number of data subjects that have not given reason for the processing ("scatter")[30] aggravates the interference. This societal dimension of privacy and data protection is also referred to as "systemic data protection."[31] In the US and Asia Pacific region, the recognition of a concept like "societal data protection" is called for, too.[32]

In the future, societal data protection interests will be harmed if police authorities use detection techniques. More objects and areas are subjected to inspection and control and there is a broadening from the traditional targeting of a specific suspect, to categorical suspicion (e.g., the computer search or video camera capturing information on all those within their province).[33] The Federal Constitutional Court of Germany dealt with such detection techniques.[34]

To this end, *police use data collections of other authorities or companies, or collect data themselves* in order to find suspects among a large group of citizens. Such automated comparison decisions are carried out for telephone data, postal mails, bank accounts, credit cards, car number plates, mobile phones, flights passengers, international banks transactions, and screenings in ID card registries.[35]

---

[29] BVerfGE 65, 1 (43).
[30] BVerfGE 120, 378 (402); 115, 320 (354 f.); 107, 299 (328).
[31] Dix in: Roßnagel, Handbuch Datenschutzrecht, München 2003; Steinmüller, Informationstechnologie und Gesellschaft, Darmstadt 1993, 671; Podlech in: Brückner/Dalichau, Festgabe für Hans Grüner, Percha 1982, 452ff.
[32] Bygrave, http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html, para. 20; Regan: Legislating Privacy, University of North Carolina Press, 1995, pp. 230ff. w. f. r.
[33] Marx: Technology and Social Control, International Encyclopedia of the Social and Behavioral Sciences, 2001, http://web.mit.edu/gtmarx/www/surandsoc.html
[34] "Verdächtigengewinnungsmaßnahme," BVerfGE 115, 320 (Rasterfahndung II).
[35] See for each data category:

- BVerfGE 113, 348 (Vorbeugende Telekommunikationsüberwachung);
- BVerfGE 110, 33 (ZKA); BVerfGE 118, 168 (Kontostammdaten); decision of BVerfG, 2 BvR 1372/07 (Mikado);

Biometric identification technologies, RFID tag systems and surveillance technologies are currently being developed.[36] The search for suspects by automatic means necessarily leads to data processing falling within the scope of Convention 108. The above-mentioned measures are possible due to automated collection of personal data. Thus, the Convention 108 **should provide for the same protection regime for data collection as for further processing.**

7 "Accountability by design"

Question 29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

As regards the accountability principle, there is no reason to exclude the public sector from accountability rules.

Question 15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Data breaches can only be avoided if compliance with the above-mentioned requirements can be verified. The principle of accountability[37] offers opportunities to evaluate police laws and specific measures for detection techniques to which large numbers of citizens are subject. For example, the respective filing systems should be designed in a way that the controller can demonstrate which data sets have been processed in what way. In particular, this demonstration could enable the controller to determine how many nonsuspects are subject to further measures. Such „accountability by design" could be ensured by defining an evaluating data field that counts the data captures, comparisons and erasures.

The value of this data field could be the basis for notification of the supervisory authority; e.g., automatically notifying the data protection authority if the number of matches exceeds a certain threshold. It is not a "data breach notification" but the notification can influence the priorities of inspections planned by of the supervisory authority. Further, the number of data sets and operations is necessary for evaluation of the legal basis and its implementation.

- BVerfGE 120, 378 (Automatisierte Kennzeichenerfassung);
- decision of BVerfG (Federal Constitutional Court of Germany), 2 BvR 1345/03 (IMSI-Catcher);
- Opinion of EDPS (European Data Protection Supervisor) on passenger name records, at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-10-18_PNR_EN.pdf;
- Opinion of EDPS on TFTP (SWIFT) II Agreement, at: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-06-22_Opinion_TFTP_EN.pdf;
- BVerfGE 115, 320 (Rasterfahndung II).

[36] Commission's summary of replies to the public consultation about the future legal framework for protecting personal data, http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf, para. 2.2.1.

[37] See for the adoption of a duty on accountability into the future Data Protection Directive, Art. 29 WP: Opinion 3/2010 (WP 173), 13.07.2010; early already according to para. 14 OECD Guidelines 1980.

This technique has to be distinguished from conventional logging.[38] The data field aggregates the processed data and counts the number of data sets that have been used for non-matches and for matches, which may cause the taking of further police measures.

The example of detection techniques shows that there is a need for accountability measures in the police sector. Further, it can be combined with the privacy by design principle. Convention 108 should **provide that, subject to the other Articles of the Convention, the designers, producers and controllers ensure that the filing system which is used for automated decisions of suspicion is designed in a way that the controller is able, on the request of the supervisory authority, to demonstrate, in an aggregated format, how many data sets have been processed and how.**

[38] For example, according to S. 14a (3) (2) HSOG (see above), logging is explicitly prohibited.

PORTUGAL – COMMISSION NATIONALE DE PROTECTION DES DONNEES

QUELQUES REMARQUES SUR LA RÉVISION DE LA CONVENTION 108

Voici quelques remarques ″impressionnistes″ présentées à titre individuel, suggérées par la pratique quotidienne et conditionnées par le manque de temps disponible (les commentaires sont présentés par rapport aux numéros des questions proposées) :

2. Il est préférable de ne pas définir (″limiter″) le droit à la protection de données, puisqu'il est complexe et composé de plusieurs facultés.

   D'ailleurs, il n'est pas équivalent au droit à la privacité : il y a des données personnelles qui n'appartiennent pas à la privacité, et il existe des aspects de la privacité qui n'ont pas de rapport avec les données personnelles.

4. On devrait pondérer si l'application de la Convention doit être absolument exclue dans les limites du domicile.

   Il peut y avoir des intromissions parentales graves dans la privacité des enfants qui devraient être réglées et contrôlées : p.e. à travers la vidéosurveillance ″domestique″; ou par le contrôle excessif des communications électroniques de l'enfant.

5. La collecte des données est aussi un traitement, qui doit être couvert par la Convention.

   V. la comparaison avec la Directive 95/46/CE

   La videosurveillance sans gravation est une opération sur des données personnelles, laquelle doit être couverte par la Convention.

7. Le principe de proportionnalité doit être expressément consacré. On l'applique, d'ailleurs, implicitement à beaucoup d'occasions.

   Il s'agit, en plus, d'un principe général de droit.

   Il est fondamental pour contrôler l'activité des entités responsables des traitements.

11. Au fond, les données sensibles le sont en fonction des circonstances et des finalités de chaque traitement.

    Par exemple, la race peut être traitée s'il s'agit de recruter des artistes dont un ou plusieurs doivent appartenir à une certaine race.

    V. les travaux convaincants de Spiros Simitis dans ce sens.

    Mais cela ne veut pas dire qu'on ne présente une énumération indicative de telles données.

12. Les données personnelles des enfants méritent une réglementation spécifique.

En tant que personnes, les enfants doivent jouir de la protection accordée à la généralité des données personnelles.

Mais le régime particulier de la Convention de l'ONU pour les droits de l'Enfant doit conduire à des normes spécifiques, aussi en matière de protection de données.

Le critère du respect pour l'intérêt supérieur de l'enfant doit, p.e, être décisif s'il existe une contradiction entre l'intérêt de celui-la et celui de son représentant légal.

La pondération de la nature évolutive de l'enfant doit, dans plusieurs situations, conduire – encore pendant sa minorité – à consulter son opinion, et, même, à exiger son consentement (p.e à propos d'essais cliniques).

Malgré l'autorité parentale sur les mineurs, la privacité de ceux-ci doit toujours être dûment respectée par les parents – p.e. en ce qui concerne l'éventuel contrôle par geó localisation.

13. Il n'est pas évident qu'il existe des avantages à consacrer le devoir de communiquer des ″ Data Security Breaches ″.

    Ce régime peut surtout se comprendre aux Etats Unis, qui n'ont pas de législation générale de protection de données.

    Et on peut même craindre que l'application de ce principe ne conduise pas les responsables à éviter de possibles sanctions, dans la mesure où on ne doit pas être admis à ″se criminaliser soi-même″.

15. Le principe ″d'accountability″ va de soi-même.

    Il est même douteux qu'il soit nécessaire, face au dû accomplissement de ses devoirs légaux par les responsables.

    En tout cas, si on veut le proclamer, il doit toujours être seulement un ″plus″ de surcroit aux devoirs déjà établis.

    On ne devrait pas chercher – ce qui n'est pas rare – à utiliser cette idée pour affaiblir les règles de protection de données aujourd'hui admises.

16. Le principe de ″privacy by design″ serait bien utile.

    D'une part, parce-que l'action de fiscalisation est toujours ponctuelle.

    D'autre part, car l'évolution des technologies surpasse souvent la vitesse de réaction des moyens juridiques.

25. On devrait non seulement proclamer l'indépendance des autorités de protection de données, mais encore spécifier les différents aspects qui doivent caractériser cette indépendance (non intégration dans l'Administration ; absence de devoir d'obéir à des instructions ou recommandations extérieures ; statut de ses membres ; budget).

PRIVACY INTERNATIONAL

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

The challenge for the Council of Europe, and for any modern legislative process, is to draft a technologically-neutral policy that is at the same time dynamic enough to reflect technological change. This is certainly possible and we propose that the convention should do this by remaining simple and concise. The term 'technology neutral', it is important to recall, focuses mostly on ensuring that law does not favour a specific technology over another, not that the law shouldn't guide the development and deployment of technologies.

2. Should Convention 108 give a definition of the ***right to data protection*** *and* ***privacy****?*

The European Convention on Human Rights already defines a right to privacy, and we don't believe that a convention on data protection should define privacy as it is likely to be limited to information processing. A right to data protection would be worth considering, as many constitutions around the world have started to state that data protection is indeed a right. See, for instance, our study on comparing privacy protections across Europe, available at https://www.privacyinternational.org/ephr

Perhaps it is more appropriate to express them as a set of broad principles.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Yes – it is important that the Convention and its principles apply broadly – any areas in which derogations from some principles may be justified need to be specific and focussed. IN particular, we believe that this comprehensive approach should be broadened to prevent arbitrary exemption under "national security". "National security purposes" must be fully acknowledged to be subject to human rights tests, including compatibility with democratic society.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely ***personal or household activity.*** *Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?*

Meanwhile, the household or domestic exemption is inapplicable to Web 2.0 in so far as it makes the data "accessible to an indefinite number of people" (Lindqvist 47). Web 2.0 typically weaves together data relating to many people, so there need to be incentives for clear and free social negotiation of norms in a plurality of contexts. For example, an exemption which risked being misapplied to social media would be unwise. However there is a legitimate exemption for a person's personal diary or "life log" or creative works – a private mental sphere. There is no reason the individual should be compelled by law to do anything with data purely of such private concern. Attempts by society to decide otherwise may be ruinous to the preservation of democracy under conditions of dramatic change in technology. That is, full application of privacy principles to the behaviour of private individuals would be onerous and oppressive – threatening other important freedoms and rights. One approach to handling this difficult issue is by the broad statements of privacy protection in the ECHR and similar human rights instruments, at the

international level. Some consideration could be given to making the privacy protections in those instruments more specific. At the national level, the issue can partly be addressed by statutorily defined rights of privacy where interpretation by the Courts has a major role, although cost and other barriers to access to courts is a significant problem. Low cost tribunals may have an important role to play.

The state does have positive duties to insure there are no impediments to individuals' exercise of "information self-determination". This will include the right to store and access data augmenting what exists in human consciousness. Just because the engineering used to create a novel subjective experience is outside the body, does not mean that the state acquires rights to inspect or interfere with that experience. It is legitimate and necessary to design systems for privacy, because computer science has shown that is the only way privacy can be preserved.

*5. The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?*

The only principle currently applying to collection is in Article 5 - that Personal data undergoing automatic processing shall be: (expressly, in (a)) "obtained and processed fairly and lawfully", and (implicitly) that data collected should be "adequate, relevant and not excessive ..." (in (c)) and "accurate" (in (d)). We submit that it would be helpful to include 'collection' in the definition of automatic processing so that all of the principles apply, where relevant, to collection. The principle needs to be strengthened by inclusion of a specific requirement that collection should not be excessive, and perhaps that it should not be by intrusive means. However, the 'data minimisation principle' (see response to Q8) is another way to achieve at least the first objective.

The definition already refers to "storage" so collection without storage implies transient processing of some kind. Often industry and other lobby groups argue than transient processing should be allowed because it is part of an "anonymisation" or "aggregration" process. Sometimes these claims are valid, mostly they are hokum. Any collection implies the possibility of retention and any creation of data must be justifiable in the context of fundamental rights.

*The definition of the **controller** of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?*

The definition is satisfactory, criteria are and should be independent and there can be several controllers for one file.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

These new definitions would only be necessary if provisions were inserted referring expressly to these entities. This may be necessary if provisions concerning 'privacy by design' are included, because it is essential that such a principle should apply to those designing equipment and not merely those utilising it, as it may be too late to factor in (or retro-fit) appropriate privacy protections once technologies are built without them. (see response to Q16)

The concept of processor is no longer useful since "processors" effectively must undertake so many duties of security and privacy compliance, that their role becomes very hard to distinguish. There is no merit in a business construct formally being responsible for privacy and security measures, but being in practice wholly dependent on vanilla terms and conditions from unregulated mass-providers of Cloud services for (especially if out of European jurisdiction).

"automated data file": The concept of "file" doesn't necessarily correspond to any functional algorithm with privacy relevance. Although it catches all, it is disconnected from logical structure. Should controllers have responsibilities to employ or eschew certain file structures, which would guarantee or preclude certain capabilities e.g. to fulfil rights? At far extreme could define properties of a "trusted computing" platform: remote attestation which demonstrated capability for privacy compliance for example might attract regulatory incentives.

"personal data": Research has shown that identifiability is "not a syntactic property" of data about individuals considered in isolation, but is only meaningful when considered for all other data. Therefore the definition of personal data cannot be fixed by reference to "identifiability" – it is inherently ambiguous whether this means "relative" to a putative controller or the "absolute" consideration all extant data held by any party. Precisely this ambiguity is the source of the most basic dysfunction in the EU Directive (and the failure to give any effect to Recital 26 – "or by any other person" - in the UK and Ireland amazingly continues to escape the Commission's explicit censure). Consider for example a national database of AC frequency in the electricity power supply: this may be used to identify the location of audio recordings. The only safe course is to widen the scope so that regulation of any processing of any data may be regulated if it is necessary to protect privacy.

Defining "manufacturer of technical equipment" may be unwise outside of a specific privacy risk and security context.

See also response to Questions 14 and 20 below for more regarding the definition of 'personal data'.

Protection principles

7. New principles could be added to the Convention, such as the ***proportionality*** *principle, which should apply to all operations carried out on the data. Such a principle is also linked to the* ***data minimisation principle*** *which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.*

These are both significant principles which could valuably be added, and we strongly support their inclusion.

Data minimisation is not really linked to the idea of proportionality. The purpose of a system defines what data is necessary. Collection or processing of this necessary minimum is not a matter of "proportionality", but of fact about which algorithms are chosen etc. Maximizing collection of data which has any plausible utility is not a legitimate activity.

"proportionality" does not have a happy history in privacy jurisprudence. It is too often used justify whatever the judge believes is right, without further inquiry, and therefore is literally irrational when applied to inherently incommensurable entities. However it may be possible to say that the effects of two alternative policies have such clear-cut difference that one is inherently more "proportionate" than another (e.g. targeted data-preservation vs. blanket data –retention).

In particular, "proportionality" cannot mean that arguments for infringing privacy are "additive" in weighing public policy justifications. Privacy could always lose any such contest, so the question arises why should it win any particular context? There is no answer to this question from the

empty rhetoric of proportionality or "balance". Independent expert technical analysis is needed of every such situation.

8. Should the question of ***consent*** *be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?*

The concept of consent is fraught with difficulty in a data protection context. If it is used it needs to be expressly defined as meaning free, informed and revocable, and not bundled with other consents. There are many current transactions which misleadingly use 'consent' when they in reality amount only to 'notice, and acknowledgement that nominated uses/disclosures are a condition of the transaction'. There should be a general principle that where genuine consent is a realistic option, it should be the preferred basis of fair processing (subject to other public interest exceptions), consistent with the overall aim of transparency in transactions involving personal data. This would be consistent with the introduction of a ' right of opposition' (see Q18) – a right to opt-out of secondary uses is necessary to avoid data controllers making them a condition of service.

It is important that any consent provision also expressly addresses the form in which consent is sought and recorded. The relevant provisions of the Canadian private sector privacy law (PPIPEDA) are relevant, as it the following proposed amendment to PPIPEDA: "the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting."

Consent should also be distinguished from voluntariness. A person does not truly consent when there is no reasonable alternative to some situation – their acts are in effect involuntarily. There may be no reasonable alternative to some Internet service which is almost essential in the modern world. Has the user therefore freely consented to the terms of use? Suppose a close examination of such terms revealed that most comparable services all contain vague and sweeping disclaimers of liability, discretion to damage the users' privacy, and do not fulfil local privacy rights? At what point are such disclaimers invalid?

However if the controller pays sufficient value, presumably most users will sell their data. Therefore the societal value of privacy may have to be protected through a democratic decision to prohibit some processing with otherwise lawful consent.

Full exercise of the possibilities of freedom also require that individuals must also be able to bind themselves irrevocably for purposes of autonomy (like Odysseus tied to the mast to resist the Sirens' song). Therefore consent not only depends on the existence of meaningful alternatives, but on whether those choices are presented fairly and comprehensibly. An effective regulator may alter market behaviour to achieve this, whilst an ineffective regulator merely camouflages the absence of true consent.

9. Should the ***legitimate processing*** *be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?*

No – fair and lawful (i.e. not unlawful), coupled with other general principles of proportionality, data minimisation and non-intrusive collection, are appropriate criteria – a list of positive grounds for processing would inevitably be incomplete.

The catalog of legitimate processing reasons in EC95/46 has created a lawyers' playground of loopholes to leap through, which has only partially been resisted through the reiteration of Art.29 WP Opinions.

This approach to legitimacy is fundamentally tautologous and unhelpful. E.g. dishonest purposes are obviously not legitimate, unless they are (e.g. deceiving a con man). Even a mundane purpose such as fulfilment of a contract begs the question of whether the system which does so is acceptably engineered to be privacy friendly.

10. Convention 108 does not expressly mention ***compatibility in relation to purpose****. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.*

Very rarely are purposes judged to be incompatible and the term has come to mean the regulator's courage modulated by the expediency of the case and the political capital at stake. It might be intended to sound reassuring, but it offers deceptively little. The question is whether the ostensible purpose is actually a subterfuge for eroding the illegitimacy of other purposes through function creep.

11. ***Special categories of data*** *which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?*

Special categories are useful, so long as absolute protection will be afforded. Unless the Convention is to specify the additional measures then there is limited value in defining 'special categories' or 'sensitive data'. Sensitivity is in any case subjective and contextual, and any list is likely to be arbitrary and incomplete. The proposed introduction of proportionality and data minimisation principles (see Q7) could replace the need for a 'special category' provision.

Even still, we must be careful. For example medical conditions, political belief, sexual practices could all be inferred from advertising and search engine data which would be classified as personal inside Europe, but which is routinely dismissed as harmlessly "anonymized" by industry lobbies, although such data many trivially be identified by statistical or procedural means.

12. A specific protection could also be applied to certain categories of data subjects. In particular, ***children*** *may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?*

For children, a vexed question is who exercises their rights on their behalf. At some variable age of maturity, children's privacy may need to be asserted against parents or guardians. It is not obvious that data controllers are in any good position to decide those questions, but clarity and certainty for the child should be paramount.

The proposed introduction of proportionality and data minimisation principles (see Q7) could adequately address the concerns about children and other potentially vulnerable groups. The explanatory materials accompanying the Convention could make this clear.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Yes, but not necessarily as part of a security principle – a right for data subjects to be informed of data breaches affecting them that meet specified threshold criteria should stand alone as a separate principle.

"Data security" is today interpreted passively as the protection of data which has been justified as lawful to process. However there ought to be a positive obligation to engineer systems to minimize privacy risk – for example by *ex ante* data minimization. Many unconventional cryptographic algorithms (such as "zero-knowledge proof") were invented expressly to allow certain functional operations to be performed with no propagation of personal data, in ways that are deeply counter-intuitive. There must be a positive obligation to design the entire system considering the full gamut of such scientific advances, not merely to protect that data which is being processed, but to minimize the privacy risk (of collection especially) for the entire system.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Yes. Such data is almost impossible to "anonymize", and so is data about social relationships. Therefore sophisticated privacy engineering methods should be aggressively applied to preclude the necessity for collection (e.g. smart metering, road pricing, authentication) and retention altogether. Location and social network data also impinges on the right of free association in society, and the right to do so privately and unobserved. Such data may implicitly constitute special category data and should be considered intrinsically toxic to privacy.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Yes – there should be an obligation to demonstrate that measures have been taken to ensure full respect for data protection rules. Caution should be taken in the use of 'accountability' which has been suggested in recent data protection debates as an alternative to specific requirements for compliance with rules. In particular, 'Accountability' cannot be and must not become an alternative to data export restrictions.

Procedural mechanisms are often a tick-box regime with no relation to actual business conduct e.g. audit standards designed for previous decades now applied to that eponymously nebulous term "Cloud computing". Technical accountability mechanisms, e.g. "trusted computing" with cryptographically subtle audit trails, offer a potentially attractive path to establishing meaningful accountability. Our concern over 'accountability' is that it doesn't appear to face consequences: a lax interpretation meaning merely a passive ability to give an account, vs. an ambiguous implica-

tion that serious consequences will follow an infraction. Serious consequences never follow "accountability" failures in privacy.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Yes, privacy by design should be expressly encouraged, although it may be difficult to operationalise this as a specific rule. A specific requirement to conduct privacy impact assessment (PIA) for major projects could help encourage privacy by design, but supervisory authorities need to be cautious about endorsing projects in advance in case it compromises their ability to subsequently investigate and enforce compliance.

The simplest way to express this is to say that if scientific discoveries prove that a service can be offered practicably in a more privacy protecting way, the adoption of state-of-the-art privacy technologies can be mandated, expressly trumping any presumed countervailing principle of "technological neutrality".

However, there is a false rhetoric of lobbyists who claim PbD is about no more than being mindful of Data Protection principles during the design of business processes. Similar lobbying battles were fought in the 1990s over the terminology "PETs", and in the 2000s over "PIAs". Mostly this lobbying was successful with policymakers – PETs and PIAs became terms which policymakers confounded with obsolete techniques with no scientifically respectable currency or relevance. Privacy-hostile lobbies now want to immunize the term "privacy by design" from technical obligations or implications.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

Yes, and it is reasonable to require that controllers' systems have this capability. Moreover all data pertaining to the behaviour of the individual must be included, and satisfactory (privacy-friendly) authentication must be pre-arranged to allow this as a minimum condition for processing such high-frequency behavioural data. Some countries may democratically prohibit such data processing altogether, e.g. the centralized accumulation of individuals' search engine histories, or Life Logs. Such Life Logging will be increasingly common (as Moore's Law keeps going) and creates an existential threat to personal autonomy in society, unless such Logs are under the exclusive and immediate control of the individual (e.g. via some personal trusted device controlling encrypted data). Technically this is achievable, but it will not be done by industry voluntarily, because the commercial inducements to centralized collection are too immense.

It is good public policy that the logic of processing should always be published and protected if necessary through intellectual property law. However the current system urgently requires reform to reject trivial, over-claimed, and submarine patents. Search engine companies will assert that they need algorithm secrecy to prevail over spammers. In such exceptional cases, the regulator may inspect the algorithms for fairness and other criteria secretly, but competition provides no reason to resist publication in principle – that is the purpose of patent protection.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

These rights are almost never exercisable in practice through access to the courts (too expensive except for celebrities). At the moment, too much depends on the diligence and disposition of the regulator.

A right of opposition in the sense used in the EU Directive (Article 14); i.e. a right to opt out of processing, should be included, even when consent was originally granted, if it is reasonable for consent to be revocable in the circumstances.

A right to oblivion (to be forgotten) needs further consideration, as there may be many circumstances in which it is unreasonable or impractical, and even conflict with other principles such as security or data integrity, or interfere with the audit trail needed for accountability.

A 'right to be forgotten' should at the very least encompass a requirement that personal data should be deleted or made inaccessible once the purpose for its collection is complete, though this does not meet all situations where such a right is needed or justifiable.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

There can be no absolute guarantee of confidentiality or integrity – only that 'reasonable measures' be taken. Supervisory authorities do however need to be much stricter in their enforcement of these principles.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

There is no need for a separate 'right not to be tracked', if personal data is defined as expressly including information about an individual's communications, location or behaviour (See response to Q14)

21. Should everyone have a right to remain anonymous when using information and communication technologies?

An absolute right to anonymity is unreasonable and impracticable in many circumstances. We do believe that it should always be the default state of affairs, and that any requirement to identify should be considered an interference that must be justified. Consideration should be given to inclusion of a principle similar to that already included in Australian privacy law as the 'anonymity principle'. Suggested wording:

> "Individuals must have the option of not identifying themselves when dealing with an entity, or of using a pseudonym, except where there is either a legal requirement for identification or where it is impracticable for the entity to deal with individuals who have not identified themselves or who use a pseudonym."

We are aware of many oppressive laws and policies emerging around the world that have made the default setting to be 'identify or you lose access to resources'. A strong statement on the importance of anonymity as the default state is absolutely essential.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

It is not appropriate for the Convention itself to try to balance every aspect of these interests, but some recognition of the public interest in freedom of expression would be desirable. This would be particularly relevant if the scope of the Convention was extended to cover individuals as data controllers (see Q4).

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

The Convention does not currently expressly provide for complaints about breaches of the principles/rules – only for remedies where requests for correction etc are denied (Article 8(d)) (check Optional Protocol?). If the Convention is to include a requirement for complaint or ADR mechanisms, then it would be appropriate for it to expressly recognise the value of representative complaints (class actions). Organisations like our own would be very interested in playing a role in filing actions.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

There may be more than one applicable law – both general and sectoral data protection laws and other laws with privacy related provisions. Insofar as data protection laws are concerned, it would be of value if, in relation to likely areas of conflict of laws, the Convention did state a choice of law rule, provided this was made subject to strong cross-border transfer rules (see Q27).

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

Supervisory authorities are only provided for expressly in the 2001 additional protocol to the Convention (CETS 181), and these provisions could usefully be incorporated in the Convention itself (see response to Q26 below). Clause 3 of Article 1 of the Protocol mandates independence, while Clause 5 requires international co-operation. It is probably not appropriate for the Convention to try to specify how these requirements are to be met.

26. Should their role and tasks be specified?

Article 1 of the Additional Protocol (CETS 181, 2001) specifies roles and functions of supervisory authorities. This should be incorporated in the Convention itself.

One particular task of a supervisory authority that needs to be spelled out is the obligation to account for their performance of their complaint investigation obligations, including by reporting to the public, on objectively determined criteria, of cases investigated (anonymised to the extent necessary to protect privacy but not otherwise), and by statistics including statistics concerning outcomes and remedies. Supervisory authorities must be able to demonstrate that they deliver remedies to complainants, otherwise their existence can simply be a cover for expanded surveillance activities. We would hope that bodies like the Council of Europe could develop assessment frameworks to ensure that this information is collected, compared, and analysed.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

It remains appropriate to require an adequate level of protection as a condition of cross-border transfer. Member states of the Convention should require that the personal data concerning their citizens is protected if it leaves their jurisdiction. The provisions of the additional protocol should be moved inside the Convention.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

'Globalisation' of 'minimum rules' is not desirable at all. It would simply be a 'race to the bottom' which would destroy any value in cross-border privacy protection. The Convention should establish the standard of protection it requires for citizens of member states, and adhere to that.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

The same basic principle of cross border transfer conditions should apply equally to the public and private sectors.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

We are not familiar with the operations of the consultative committee and have no particular opinion on this question.

SENEGAL - COMMISSION A LA PROTECTION DES DONNEES

Objet et champ d'application de la Convention, Définitions

1. Rédigée selon une approche « technologiquement neutre », la Convention 108 est un instrument général et simple : peut-on conserver cette approche ou doit-on au contraire élaborer un texte plus détaillé ?

A mon avis, il est important de conserver cette approche. Si on définit de manière limitative le champ d'application de la Convention en listant les technologies concernées, on sera amené à légiférer périodiquement face à l'apparition nouvelles technologies ou simplement face à la convergence de celles-ci.

*2. La Convention 108 devrait-elle définir le **droit à la protection des données** et le **droit au respect de la vie privée** ?*

Ni l'un ni l'autre. Je pense qu'on devrait élargir le droit qu'on cherche à protéger en définissant dans la Convention le « **droit à la protection des données et de la vie privée** ». La protection des données est associée à celle de la vie privée ou inversement. Par conséquent, il serait plus pratique de les associer dans la même définition. Le droit commun applicable à la vie privée est fortement influencé par les technologies.

3. La Convention 108 protège les individus contre toute atteinte portée à leur vie privée par des autorités privées et publiques, y compris la police et la justice. Cette approche globale doit-elle être conservée ?

Oui, l'enjeu étant d'assurer une protection globale de la personne physique.

*4. La Convention 108 n'exclut pas de son champ d'application les données traitées par une personne physique pour l'exercice d'**activités exclusivement personnelles ou domestiques**. Doit-on maintenir cette approche, ou au contraire introduire une exception dans ce cas précis (dans le contexte spécifique du Web 2.0.) ?*

Cette exclusion est doit être mentionnée dans la Convention dans la mesure où les autorités de protection ne peuvent pas s'occuper de tous les types de traitements. C'est une disposition qui pouvait être élargie en y ajoutant « les traitements dont les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ».

*5. La définition du **traitement automatisé** n'inclut pas la collecte des données : le fait que la collecte fasse l'objet d'une disposition spéciale est-il problématique ? Est-ce suffisant ? Doit-on ajouter d'autres opérations à la liste existante ?*

La question de la « visualisation » des données personnelles notamment celles des scanners corporels dans les aéroports mérite réflexion. Je pense qu'on devrait considérer les images des scanners corporels comme des traitements automatisés bien qu'il n'existe pas à proprement parler un traitement classique des données.

*La définition du **maître de fichier** devrait être revue : plusieurs critères doivent-ils être répertoriés, ces critères doivent-ils se cumuler, peut-il y avoir plusieurs maître de fichier pour un seul fichier?*

Oui, il est possible d'avoir plusieurs maîtres de fichiers : le responsable en tant que chef d'entreprise et le responsable technique en tant que gestionnaire des données. Il convient donc de préciser les fonctions du maître de fichier en parlant de « maître de fichier chargé de la collecte et du traitement » ou « maître de fichier en tant que personne morale de l'entreprise ou de l'administration ».

*6. De nouvelles définitions sont peut-être nécessaires, comme celle du **sous-traitement** ou celle du **fabricant des équipements techniques**.*

Principes de protection

*7. De nouveaux principes pourraient être ajoutés à la Convention, comme le principe de **proportionnalité** qui devrait s'appliquer à l'ensemble des opérations réalisées sur les données. Ce principe est également lié au **principe de minimalisation des données** qui vise à limiter la collecte des données à caractère personnel au strict minimum, voire à y mettre un terme quand cela est possible.*

Oui, c'est pertinent.

*8. La question du **consentement** devrait-elle être envisagée en étroite liaison avec le principe de transparence et l'obligation d'informer, ou en tant que condition nécessaire à satisfaire un traitement loyal et licite avant toute autre action ?*

Le consentement suppose d'être au courant du traitement (obligation d'informer) et d'avoir confiance à cause de la politique de transparence des gestionnaires. Donc, il est impératif de concilier les deux principes : consentement et droit d'informer.

Par ailleurs, le débat doit porter maintenant sur le traitement de certaines données qui doit être obligatoirement soumis au consentement des personnes concernées. L'exigence du consentement condition nécessaire pour le traitement loyal et licite, doit être réservée au traitement d'une catégorie de données.

*9. La Convention 108 devrait-elle aborder la question de la **légitimation des traitements de données** comme le fait la Directive 95/46 dans son article 7 ?*

Oui, fondamentalement.
Faudrait-il dresser une liste de fondements légitimes pour le traitement des données ?

*10. La Convention 108 ne fait pas de référence expresse à la **compatibilité nécessaire entre l'utilisation des données et le but** initial de leur collecte. Or, aujourd'hui, les données à caractère personnel sont généralement utilisées à des fins qui vont bien au-delà de celles initialement prévues, d'où la question de la compatibilité.*

Sans la compatibilité, il est difficile d'assurer une protection efficace aux données collectées. Donc, il convient de corriger ce manquement.

*11. La définition des **catégories particulières de données** faisant l'objet d'une protection accrue est très large, ce qui pourrait entraîner une application excessive de cette restriction : est-ce l'information ou son traitement qui est sensible ? Devrait-on ajouter d'autres catégories de données, comme les numéros d'identification (nationaux) et les données biologiques ou biométriques ?*

C’est l’information qui est sensible et non le traitement.
Oui pour qu’on ajoute les données biologiques ou biométriques.

12. Une protection spécifique pourrait également être appliquée à certaines catégories de personnes sur lesquelles portent les données. Les ***enfants,*** *en particulier, peuvent avoir besoin d’une protection spéciale en raison de leur vulnérabilité. Y-a-t-il un besoin de dispositions spécifiques à la protection des enfants ? Si tel est le cas, quels aspects devraient aborder ces dispositions ?*

Je suis d’accord pour des dispositions spécifiques en vue de renforcer la protection des données des enfants. Les aspects à prendre en considération peuvent être notamment : les conditions de collectes des données des enfants, leur traitement et leur transfert. Sur le plan technique, des mesures doivent être exigées aux responsables des traitements.

13. L’article 7 de la Convention porte sur la ***sécurité*** *des données au sens restrictif du terme, à savoir la protection contre la destruction accidentelle ou non autorisée, la perte accidentelle et l’accès non autorisé, la modification ou la diffusion. La notion de sécurité devrait-elle également inclure un droit pour les personnes concernées d'être informées des violations de la sécurité des données ?*

Je suis pour le droit d’informer les autorités étatiques (Police et justice) et de contrôle (commission de protection des données personnelles) et non les personnes concernées. Ces dernières ne peuvent rien faire face à ces violations de la sécurité. Au contraire des autorités susmentionnées.

14. Il existe certains risques découlant de l'utilisation des données de ***trafic et de localisation*** *(données techniques accompagnant une communication) car ces données peuvent révéler les mouvements, orientations, préférences et associations avec d’autres. Avons-nous besoin de règles particulières pour l'utilisation de ce type de données ?*

Un minimum de règles doit être prévu dans la Convention.

15. Faut-il mettre en place des systèmes de ***responsabilisation,*** *ainsi qu’une obligation de prouver que des mesures efficaces ont été prises pour garantir le plein respect de la protection des données ?*

L’approche de la contractualisation peut être utilisée pour mieux responsabiliser les gestionnaires des données à caractère personnel.

16. Devrait-on appliquer le principe du « ***respect de la vie privée dès la conception »*** *(Privacy by Design) qui vise à prendre en compte la question de la protection des données dès le stade de la* ***conception*** *d’un produit, d’un service ou d’un système d’information ?*

Il est impératif de prévoir cette possibilité. C’est l’un des moyens pour assurer le respect de la vie privée dès la conception d’un produit. Le principe doit être posé dans la présente Convention.

Droits – Obligations

17. Le ***droit d’accès*** *ne devrait pas se limiter aux données mais devrait couvrir l’accès à l’origine des données, c’est-à-dire la personne qui est à l’origine de la communication. Ce droit devrait-il également couvrir l’accès à la* ***logique*** *du traitement ?*

*18. Le **droit d'opposition** se justifie dans les cas où le traitement des données ne repose pas sur le consentement de la personne concernée. Le lien entre droit d'opposition et droit à l'oubli pourrait être examiné, ainsi que la possibilité de garantir le respect et l'exercice de ce droit.*

Tout d'abord, il faut définir le droit à l'oubli.

Ensuite, le respect du droit à l'oubli doit être exigé en application du principe relatif à la finalité du traitement. Ce qu'il faut renforcer, ce sont les conditions d'application du principe de finalité. En respectant le principe de finalité d'un traitement, la question du droit à l'oubli ne se posera plus.

19. Devrait-il y avoir un droit qui garantisse la confidentialité et l'intégrité des systèmes d'information ?

Oui, les grands principes être posés dans la Convention.

20. Faudrait-il introduire le droit de tout individu à « ne pas être localisé / tracé» (identification RFID) ?

21. Les utilisateurs des technologies de l'information et de la communication devraient-ils avoir le droit de rester anonymes ?

Oui, dans une certaine mesure.

22. La Convention 108 devrait-elle aborder la question du juste équilibre entre la protection des données à caractère personnel et la liberté d'expression (nouveau concept de la presse et du journalisme dans le contexte du Web 2.0.) ?

Sanctions et recours

23. Devrait-on introduire des recours collectifs dans la Convention ? Faut-il examiner l'introduction d'autres mécanismes de règlement des litiges ?

Droit applicable en matière de protection des données

24. Doit-on envisager une règle qui déterminerait le droit applicable au traitement des données (dans les cas où différentes juridictions sont concernées) ?

A mon avis, le droit applicable au traitement des données doit être celui dont dépend la victime. Ce principe peut être inscrit dans la Convention.

Autorités de protection des données

25. Comment garantir leur indépendance et assurer une coopération internationale entre les autorités nationales ?

Il faut conserver et renforcer le système des autorités administratives indépendantes. En ce qui concerne la coopération internationale entre les différentes autorités, l'idée d'une autorité supra nationale peut être envisagée.

26. Faut-il spécifier leur rôle et leurs missions ?

Seulement les grands principes.

Flux transfrontières de données

27. La Convention 108 avait pour but de concilier la protection effective des données et la libre circulation de l'information sans considération de frontières. Ces principes ont été développés plus avant dans un protocole additionnel (STCE 181, 2001). En principe, un niveau de protection adéquat doit être assuré.

28. Doit-on entièrement réexaminer la notion de « flux transfrontières de données » à l'heure d'Internet, où les données circulent instantanément à travers les frontières ? Serait-il utile de fixer des règles minimales internationalement reconnues pour garantir le respect de la vie privée sans considération des frontières ? Quel pourrait en être le contenu ?

Oui. Il faut consacrer les droits fondamentaux de l'Homme virtuel.

29. Doit-il y avoir des règles différentes pour le secteur public et le secteur privé ? S'agissant notamment du secteur privé, doit-on avoir davantage recours à des règles d'entreprise contraignantes, éventuellement associées à un système de responsabilisation du destinataire final pour garantir le respect de ces règles ?

Rôle du comité consultatif

30. La Convention 108 a créé un comité chargé de faciliter son application et, le cas échéant, de l'améliorer. Doit-on renforcer le rôle jusqu'ici principalement consultatif du comité ? Si oui, quelles fonctions faut-il développer plus avant : l'activité normative, le règlement des litiges, le suivi ?

SPYROS TSOVILIS

Fonctionnaire du Conseil de l'Europe, ancien Secrétaire du Comité de la Convention 108.

Protection des données, nouveaux défis, réforme et coordination CdE/UE

La protection des données se trouve de nouveau à un carrefour de son histoire, un tiers de siècle après sa création : d'un côté le **défi des droits fondamentaux à l'épreuve des nouvelles technologies** (Internet, Réseaux sociaux, Téléphonie mobile, etc…), de l'autre côté, **le défi des normes européennes à l'épreuve de la mondialisation** (applicabilité des normes démocratiques, techniques et flux transfrontières de données à d'autres pays non européens).

En effet, la protection des données a d'abord **un contenu politique** : elle a signifié la reconnaissance pleine et entière que si pendant longtemps les Etats opéraient en secret et les individus se devaient d'être transparents – avec les excès que l'on aura connu, non seulement hélas dans la littérature mais bien dans la réalité politique des régimes autoritaires – dans une démocratie, l'Etat se doit d'être transparent et les individus ont droit au respect de leur vie privée. La protection des données est intimement liée à la conception qu'ont le pouvoir et les citoyens de l'information.

Ce premier aspect de la protection des données revêt une actualité nouvelle, par exemple, au vu des **aspirations démocratiques qui ont surgi parmi les citoyens de certains pays** qui ont souhaité secouer le joug des méthodes d'exercice traditionnel de pouvoir, notamment dans des états de police. Il convient d'adopter au plus tôt de bonnes pratiques en matière de gestion de l'information et de données personnelles dans les pays en transition démocratique. En même temps, les garanties offertes par la protection des données connaissent une remise en cause en raison d'un renforcement des **politiques sécuritaires** en Europe, des défis de la lutte contre le terrorisme ou la criminalité organisée, mais aussi des pressions en matière de **restrictions budgétaires**, conduisant parfois à la remise en cause de certains acquis démocratiques ou sociaux.

Le développement des technologies et des capacités des administrations (ex : santé, sécurité sociale, fiscalité), des personnes privées, de certaines professions (ex : médecins), d'entreprises (ex : assurances, banques, télécommunications) ou de multinationales, de traiter de manière automatisée un nombre considérable de données personnelles, notamment à des fins économiques et/ou commerciales, fait appel à l'autre volet de la protection des données : l'exigence de solidarité et de respect de la dignité humaine et des droits fondamentaux des personnes face à la **recherche accrue et systématique de profits et de compétitivité économiques** au moyen du traitement de telles données, notamment dans le contexte **de la mondialisation**.

Les produits issus des nouvelles technologies et de la « convergence » d'une part et la révolution des mœurs proclamée par les adorateurs des réseaux sociaux d'autre part, conduisent à interroger de manière urgente la **pertinence des normes fondamentales de la protection des données et leur application en pratique**. Par exemple, quelle est la pertinence du principe de finalité sur Internet, avec l'explosion des usages multiples des téléphones portables, des réseaux sociaux, quelle est la réalité du droit d'accès des personnes aux données les concernant, quelle est la valeur du consentement…

Les révolutions opérées sous nos yeux dans les pays du sud de la Méditerranée et l'opportunité pour l'Europe de soutenir les aspirations démocratiques des citoyens des pays tiers, mais aussi la nécessité pratique (qui est en même temps une obligation conventionnelle) de **promouvoir le flux transfrontière de données le plus libre et le plus sûr possible**, justifient la prise d'initiatives appropriées et l'élaboration de politiques ambitieuses et coordonnées au niveau européen.

Les défis posés par la protection des données illustrent **l'action coordonnée** que peuvent mener ensemble le CdE et l'UE – dans le sillage du Programme de Stockholm – pour **promouvoir des normes qui ont un caractère universel** : tout être humain souhaite pouvoir communiquer et s'exprimer librement soit en donnant la plus grande publicité à ses propos (par exemple en les publiant sur un « mur »), soit au contraire en sachant pouvoir compter que le secret des ses communications privées est garanti par la loi et dans la pratique.

Le CdE offre le cadre général d'une coopération de tous les pays disposés à respecter les mêmes normes en matière de protection des données, sur un pied d'égalité, et d'une union possible de leurs efforts sous les auspices de la Convention STE n°108 [305] qui est ouverte à l'adhésion de tous. Mais **il a besoin de l'UE comme partenaire** pour sa puissance d'inspiration normative, son accompagnement en termes de moyens de renforcement de la mise en œuvre et de contrôle des normes de protection des données. La crédibilité des normes en matière de protection des données se trouverait d'ailleurs renforcée de manière générale si les pays qui utilisent le plus les nouvelles technologies (ou qui brassent le plus grand nombre de telles données et qui sont soucieux d'offrir à leurs citoyens un environnement où l'information participe à leur émancipation et non à leur aliénation), rejoignaient le CdE et l'UE dans leurs efforts. Le CdE et l'UE, ensemble, doivent œuvrer pour que de tels **pays tiers,** à commencer par les Etats-Unis, le Brésil, l'Argentine, l'Afrique du Sud, l'Egypte, la Tunisie, l'Inde, l'Australie, la Corée du Sud et le Japon, ratifient, dans un avenir proche, la Convention STE n°108.

Une telle réactivation de la Convention du CdE impliquerait alors la mise en place d'un réel **suivi du respect par les Parties des normes** communes. Cela aussi devrait être une exigence tant du CdE que de l'UE, non seulement pour la crédibilité de leur système normatif (pour que les dispositions en matière de protection des données soient appliquées et que l'échange transfrontalier de données puisse être opéré conformément au droit en vigueur, de la manière la plus libre et la plus sûre possible), mais aussi parce qu'aucun Etat tiers ne voudra se plier ou incorporer une directive européenne sans contrepartie ou garantie de réciprocité, alors qu'il peut accepter d'être lié par un Traité commun auquel il est Partie à part entière, sur un pied d'égalité.

Ce suivi comprendrait, notamment : la vérification de la législation générale et particulière (banques, assurances, emploi, santé, police, justice, etc…) ; la vérification des moyens des autorités de contrôle ; la réalité en pratique de l'exercice des droits des citoyens ; les obstacles éventuels à un libre flux transfrontière de données. Il s'exercerait en étroite coopération avec l'UE et au moyen de procédures dont l'efficacité a déjà été démontrée au sein du CdE.

Les défis que soulève la protection des données sont une **opportunité** unique pour le CdE et l'UE de créer une manière de coopération nouvelle, plus poussée, pour renforcer la cohérence de l'ordre public européen et pour réactiver l'intérêt des Etats non-membres de l'UE à œuvrer ensemble dans le domaine de la protection des données. Les travaux de réexamen de la Convention STE n° 108 – en vue de son adaptation éventuelle – proposés par le Secrétaire général du CdE sont là aussi une opportunité unique pour inviter les Etats tiers non-européens mentionnés plus haut à participer au stade le plus précoce et sur un pied d'égalité à la rédaction ou réaffirmation des normes communes et des moyens de suivi de leur application.

[305] La référence à la Convention STE n°108 doit s'entendre comme incluant ses protocoles d'amendement et additionnel.

TECHAMERICA EUROPE'S

TechAmerica EUROPE

THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

TechAmerica Europe's contribution to the public consultation on the modernization of the Convention 108

Brussels, 10 March 2011

TechAmerica Europe represents leading European high-tech operations with US parentage. Collectively we invest Euro 100 bn in Europe and employ approximately 500,000 Europeans. TechAmerica Europe Member companies are active throughout the high-technology spectrum, from software, semiconductors and computers to Internet technology, advanced electronics and telecommunications systems and services. Our parent company, TechAmerica (formerly AeA and ITAA), is the oldest and largest high-tech association in the US.

TechAmerica Europe would like to thank the Council of Europe for the opportunity to provide its contribution to the public consultation on the modernization of the Convention 108. Data protection, privacy and security are fundamental issues for our member companies and we hereby look forward to continue to provide concise, technical and timely information as well as enhancing dialogue between CoE decision makers and leading technology companies.

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

TAE supports the technology-neutral approach taken in Convention 108 and believes it is important that this approach is maintained.

Given the fast pace at which technology continues to develop, TAE believes legislation should not attempt to run behind technological innovations but instead provide an appropriate and flexible legal and regulatory framework to support the continued development of new technologies. It is Important therefore that technology neutrality in the Convention is maintained to ensure the framework is flexible in order to easily adapt the rules to new technologies and applications and not inhibit or prevent innovation in the future.

2. Should Convention 108 give a definition of the right to data protection and privacy?

The current Convention outlines upfront the importance of respecting the rights of individuals' privacy in light of the processing of personal data. Given that the Convention's current text has provided clarity on its purpose and role since back in 1981 it is not seen as necessary for a

further definition to the included at this time. If a definition is to be proposed it is important that this remains technology neutral and principle based.

Where further clarification on the definitions used in Convention 108 may be however Council of Europe should bear in mind that the Convention's current definition of personal data now operates in an age where information that may, or may not, identify an individual, is diversely located and being processed by a number of different organisations in various locations and across different technological platforms, systems and even devices. Therefore while the definition as defined is supported by TAE, there are concerns as to how this definition could be interpreted and applied differently by many countries and the need to ensure there is ongoing legal certainty as to how the current definition should be interpreted which is crucial for business and the enablement of global data flows.

Due to the technical and legal complexities that may arise in practice with a possible revision of the definition of personal data, TAE calls on the Council of Europe to discuss in detail further with industry any proposals to change the Convention's definitions before moving forward.

3. Convention 108 protects against privacy intrusions by private and public authorities including law enforcement. Should this comprehensive approach be retained?

Clearly one of the main drivers of the current review of the overall EU data protection Directive (95/46) is the impact of the Lisbon Treaty on the legal structure on data protection in the EU. With the disappearance of the pillar structure, there is a need to work on a holistic framework covering both the law enforcement side as well as the commercial environment.TAE realizes that not all legal rules can apply simultaneously to both sides (private and public sector as well as law enforcement) and envisages instances where there should be different rules, partly, for public authorities and private entities. However, it is clear that the same underlying principles and requirements of transparency and process for data protection should apply to both sectors.

As the current approach of the Convention already takes such a holistic based approach it is considered to be appropriate and should be retained at this time. However, it is recognised that as the review of Convention 108 continues the introduction of new concepts and proposals may raise additional issues that need to be considered further regarding to what extent the same data protection rules and requirements should apply to law enforcement bodies as to all other bodies. This will be particularly important given many of the proposed changes being discussed and how some of the new concepts being proposed might be impacted.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web2.0.)?

It is not clear what benefit a move to exclude certain types of data from the Convention would bring and also how such a move would be implemented, communicated and ultimately understood by individuals particularly in the online environment.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list? The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?

Current definitions of data controller and data processor are terms that are understood by both private and public sector bodies and well integrated into organizations business practices. A review of Convention 108 should not seek to alter, remove or replace these well understood terms or seek to remove the fundamental distinctions between data controllers or data processes.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Any introduction of definitions related to technical equipment could not only impact or endanger the technology neutrality of the Convention but could also mean that the Convention may become quickly out of date as technological equipment and solutions tends to develop and evolve faster than legislation.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

TechAmerica Europe considers that the introduction of new, not yet defined principles or concepts would need further and thorough debate before considering its possible inclusion. For example further clarification and understanding would be needed on how any proportio-

nality principle might be defined before TAE can provide any comment on this suggestion. As data minimisation already plays an important role in the data protection legal framework and continues to be supported by TAE as just one of the technological approaches and solutions that can be deployed to manage data privacy and security. There are some concerns about the Council's proposal to further enhance the role of data minimisation in the Convention as this could be seen as highlighting a specific technological approach over other approaches to achieving effective data management. It is rather suggested that the Council considers the role that self-regulatory measures and best practices could play to encourage and support the increased take up and use of data minimisation in general. In fact, it is not completely clear what outcome is being sought by creating a principle of data minimisation. It should be noted that data minimisation requires a full understanding of the data in question, in order to delete with full confidence. An obligation to data minimisation may therefore require additional steps in collecting, processing and controlling data flows.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Given citizens' concerns over the privacy and security of their information, the focus given to transparency in data processing is understood. However, given a possible proposed introduction of a principle in this area, further clarity and details are needed on how transparency would be defined and what might be required to demonstrate compliance with such a principle before it can be fully supported.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

The broad principle based approach and use of common concepts has enabled the Convention to remains sufficiently flexible, technological neutral and adaptable by EU Member States as well as other non EU countries. This approach is supported by TAE and should continue. Moves to introduce more specific measures (such as lists) or requirements for particular aspects, such as data processing, could prevent the Convention from remaining flexible enough to be adaptable to new technologies and applications that will emerge in the future to protect data privacy and security.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

It should be noted that first European Breach notification regime was introduced in the review of the ePrivacy Directive (2009/126) as a move to increase levels of data security and raise awareness, and reassurance, amongst citizens across Europe of how their personal data is being secured and protected. To achieve a similar aim in the review of Convention 108, it is seen as fully appropriate that the review considers measures that might increase transparency for citizens.

A discussion on a horizontal breach notification regime, applied to all sectors (both public and private) which process and store individuals' personal data could be one possible option. However, any requirement introduced would need to be appropriate and non burdensome to either businesses or citizens.

If a breach requirement was to be introduced, further discussion would be needed with industry, in order to determine what would be considered as a serious breach, then to set an agreed level (which could be related to financial impact or reputational loss for example) for when a breach would be serious enough to trigger a notification requirement and finally to define the action required, as well as when notification is to occur and to whom, but also recognises the important proactive role data privacy and security technologies such as encryption can play.

Given that the EU has already taken its first steps towards a data breach notification with the review of the ePrivacy Directive, TAE suggests that the Council considers the approach already taken and seek to avoid a proliferation of different regimes, and ensure as much consistency as possible in the development of any general breach requirement.

Any proposal for a breach notification system applicable to all businesses and organisations should be carefully crafted to prevent the issuance of immaterial notices, principally through the adoption of an appropriate standard of harm for triggering notice and an exception for technical protection measures. The right balance must be found between notification as a mean to improve appropriate security measures and sanctions versus remedial actions implemented in order to minimize harm, disruption and reputational consequences. In this context, entity or group internal disclosures should be explicitly excluded as unauthorised disclosures.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data ?

Convention 108 currently operates in an age where an increasing amount of different types of information that may, or may not, identify an individual, is diversely located and processed by a number of different organisations in various locations and across different technological platforms, systems and even devices. However, it is important to recognise that there are different types of data being processed and not all data will be capable of identifying an individual preferences or movements or even identity. For example it should be remembered that traffic data is technical information only which is used to convey messages over an electronic communications network such as the internet. As a result on its own traffic data cannot alone be used as an identifier and will for many processors of traffic data simply be technical information. Traffic data may only be able to identify an individual when it is used in conjunction with other data that a specific provider may have access to.

The reality is that traffic data is being used by different organisations for many different purposes which can range from marketing, billing, interconnections as well as for providing up to date online security and privacy. Given that this technical information is being used in different ways, the level of data protection required for traffic data may also depend on whether the traffic data is being used in a particular way. Therefore the introduction of specific rules relating to the processing and protection of traffic data would not only be difficult to define but also implement given traffic data's varied role and use. The introduction of specific rules in this area could also introduce additional burdens or barriers to the processing of traffic data which is essential technical information needed to deliver online services such as internet security for European citizens, businesses and governments. Without the ability to process traffic data. For example EU citizens computers could fall victim to hackers and viruses which would also put at risk the ongoing data protection and privacy of online information.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

TAE understands accountability, as an underlying principle that could encompass existing business practices (such as Privacy Impact Assessments or more informal internal controls or the appointment of privacy officers) in a move from an ex ante regime to an ex post legal framework. In an ex post system, organisations (public and private) are accountable for their handling of data, wherever that data travels instead of merely seeking legal compliance. Ensuring that this accountability follows the data, regardless of where it is controlled or

processed, will ultimately benefit all citizens. It is however broader than only focused on increasing the data controllers' responsibility as mentioned in the Communication. It is a concept that underpins the entire legal framework, on how we look at data protection, on how we enforce and supervise it.

TAE therefore would support an accountability principle if defined as an ex-post, enforcement-based approach rather than an ex ante compliance-based approach.

However, introducing only a principle will not increase the accountability of organisations as it should be part of a holistic approach and has many aspects that need to be looked at, such as how to demonstrate and measure accountability. There are many elements of an organisation's processes to demonstrate accountability but it should be clear that there is no one way. Different organisations with different processes might have distinctly different accountability mechanisms. The Council should therefore avoid too descriptive and mandatory elements of accountability but could discuss with stakeholders how to further implement this. As a move to an *ex post* system could lead to a system with increased requirements for organizations to demonstrate certain behavior, and more responsibility also for regulators, it is necessary to study the impact carefully.

The move of the legislative framework to an *ex post* environment would not only provide more clarity to data subjects and controllers, it would also be an opportunity to reduce unnecessary administrative burdens that do not contribute to a better data protection for the subjects. It is equally important to note that the introduction of an accountability based compliance model does not also unintentionally create additional administrative requirements or burdensome data protection provisions that will not benefit the consumers, businesses or economy and competitiveness.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

The introduction of a "Privacy by Design" concept is welcome, but much further clarity is sought on how it would be defined or implemented before it can be fully supported. However, Privacy by Design should by no means be a technology-specific requirement for privacy enhancing technologies to be embedded within products in the design stage. Indeed, this would go against technological neutrality. It should focus on ensuring that the appropriate process controls are in place to guarantee the privacy and security of the data.

Privacy by Design is a process that organisations should complete at the start of a project and reassess regularly to ensure that the data privacy and security measures are applied from day

one and remain appropriate over time. Such a process is an opportunity to enhance the technological and organisational measures required from organisations to ensure data privacy and security.

While technology is clearly an enabler to increasing data privacy and security, it is important that any requirement introduced remains procedural and not technology specific. Moreover, Privacy by Design should be understood as the objective/outcome sought. However, the means towards that end should be best determined in each individual case by the data controller. Additionally, Privacy by Design could also encourage greater take up and use of Privacy Enhancing Technologies ("PETs") as means of supporting compliance with the Privacy by Design procedural requirement.

PETs as a concept may be a useful tool and their promotion is encouraged in the context of Privacy by Design, with a focus on highlighting examples of best practices and benefits. However, PETs should not become legal requirements: depending on the information they process and the business model they follow, organisations across different sectors should be afforded sufficient flexibility to determine how best to comply with data protection rules, thereby ensuring the most effective protection for data subjects. Greater promotion of PETs is therefore supported as a part of the toolkit for companies implementing a process-based concept of privacy by design.

Rights – Obligations

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

While clearly the right to have data deleted already exists in the overall data protection legal framework across Europe, any move to introduce new, as not yet defined concepts, such as a right to "oblivion" would need to be carefully considered and discussed at length before moving forward. If however what is being envisaged is related to the proposed inclusion by the European Commission of a "right to be forgotten" in the overall data protection legal framework then TAE believe this proposal warrants further clarification and discussion. TAE would like to better understand if a proposal in this area is to be taken forward, the parameters of what constitutes "user data" that might be affected by a right to be forgotten, or oblivion, are carefully and clearly defined, by excluding business data that is reasonably accessible in the ordinary course of business, for example metadata created by the service provider.

Also how would the implementation of such a right impact backup databases (both at controller and processor levels), and how would this right co-exist with the current data retention obligations and requirements for data access rights for law enforcement? Clarification is also needed on what level of deletion is needed. It will certainly depend on the sensitivity of personal data, if shredding or overwriting the storage media would be required.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

Convention 108 was originally introduced in an era prior to the full rise of the Internet era and the convergence of ICT technologies, when the risk related to data protection was limited to offline filing systems and computer mainframes operating on nationally protected computer networks and systems. However, Europe is now immersed in a globally networked society where personal data, like other types of data, is collected, correlated, amended, shared and reused across many different systems that are increasingly interconnected. In addition the increased globalisation of data comes with both increased benefits but also risks for personal information. Personal data continues to be a key target for cyber criminals due to the value attached to information and has therefore the systems that personal data is stored, processed and accessed are at greater risk from phishing, spam and identity theft related attacks. The security, confidentiality and integrity of information systems involved with personal data therefore remain important to maintain and that appropriate technical and security measures are introduced to protect the privacy and security of data whenever and wherever it may be being accessed, shared or processed. In addition different types of data, for example traffic data, personal data and/or sensitive data, may also require different levels of protection and security.

Therefore Article 7 of the Convention that currently requires appropriate security measures to be taken to protect personal data continues to be seen as important and should be maintained. It could however be further enhanced by recognizing the need to ensure the security measures are regularly assessed and updated based on an analysis of the risks to the data to ensure that the measures introduced remain relevant and appropriate.

It is suggested that any proposals to address the confidentially and integrity of information systems should be carefully considered and discussed with industry before moving forward to ensure that any proposals remain technology netural and do not prevent industry from developing and implementing appropriate technical and security measure to protect information systems as the amount of data being processed increases and the online threat environment continues to evolve and risks to personal data , as yet unidentified, emerge.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

TAE agrees that data subject's right to data access and to have delete data are important tools in a data protection legal framework that empowers individuals and increases transparency of how data is being. However, a move in towards introducing a right to be anonymous raises a number of questions around the potential consequences and risks such a move may bring. For example, if data is anonymised already what level of anonymisation might be required? How would such a right to be anonymous be exercised in relation to metadata or profiles put together on the basis of previously collected data that may be subject to this right? Also how would the implementation of this right impact backup databases (both at controller and processor levels), and how would this right co-exist with the current data retention obligations and requirements for data access rights for law enforcement? Clarification and further discussion would also be needed on what level of deletion may be needed. It certainly depends on the sensitivity of personal data if shredding or overwriting the storage media would be required.

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

The proposal for class action to be introduced should not be entered into without clear evidence that it is either necessary or appropriate at this time. Not only is there no evidence of the demand by citizens for such a right of action the consultation does not provide any clarify as to the situations being envisaged where a right to action might be able to be applied. Given that data protection authorities already have their own procedures and processes for investigating non compliance with data protection laws, and if appropriate, to bring sanction upon organisations that have been found to be non compliant TAE therefore urges the Council to provide evidence as to specific demands from citizens for the ability to take such action. There is also a need for data on the number attempts to bring of similar cases that have been attempted to be brought before the courts in order to demonstrate that this right is in fact required or even needed in Europe. Without demonstrating such evidence, this proposal should not be taken forward.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

It is important that there is a coherent interpretation of the legal framework across all signatories. The harmonisation of law is a key tool to enabling operations on the global market and helping companies to operate in multiple Member States.

TAE would like to see the review examine the benefits of introducing a legal principle in the framework that would clarify which Member State law applies, if a legal dispute arises and is related to the data protection legal framework. One of the possible ways of ensuring legal clarity is the introduction of a Country of Origin requirement, as used in the e-commerce Directive, so that the applicable data protection law is the law of the Member State where the organisation is formally established. This approach could also help to address jurisdictional issues related to the emergence of cloud computing services. However, any changes to the rules on applicable law should be thought through extremely carefully, given the potential impacts not just to the relations between businesses and consumers, but also in the relations between businesses and government authorities, including law enforcement authorities.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?26. Should their role and tasks be specified?

Given the role they play TAE is supportive of the independence of data protection authorities. Moves that would see greater cooperation and coordination in their activities woudl also be supported. For TAE see greater mutual recognition of measures by DPA (such as possible standard privacy notices or notification forms) as key to achieving harmonization in the application of data protection laws and simplify administrative burdens.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured. 28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

It is recognised that there are clearly inconsistencies with the current rules regarding international data transfers that must be addressed. Today's citizens participate in a physical and virtual world which means that data crosses jurisdictions' borders at a click of a button possibly to non-EU countries that may in fact fail the adequacy test outlined in the current EU Data Protection Directive (95/46). As a result, the adequacy principle is seen to not be working.

The proposal to reconsider how international data moves and is seen as an opportunity to also consider whether the adequacy principle still has a role to play. TAE would urge the Council to examine this issue in more detail and use this opportunity to consider other possible approaches that could replace the adequacy principle. For example how it may be possible for companies to certify their handling of data on a worldwide basis under the condition that the parent company agrees to ensure that safeguards are put in place for the processing of the data. It is suggested that such an accountability focused approach to international data governance may be more preferable and more workable than trying to make the adequacy principle fit.

A system based on a principle of "accountability" as a viable basis for transferring of data out of the EU. Under such a system, each data controller would be held responsible for understanding the risks to data under its control and for ensuring the protection of that data regardless of its location. Such an approach would emphasise compliance with substantive principles of data protection law rather than specific, prescriptive rules.

There have already been positive moves in this direction such as the evaluation processes inherent in the binding corporate rules (BCR) process. The BCR approval process could be looked at in more detail as an example of how such an approach could be introduced. This would also be an opportunity for the Commission to consider how BCR could be improved by making sure it is less burdensome, complex, costly, time and resource demanding procedure, not limited to intra-group transfers, included transfers to processors and ensure there is a higher level of transparency regarding the additional DPA requirements at national level.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

BCR is a useful tool and an interesting concept also in the fame of the discussion on accountability. BCRs are already applied under the EU data protection regime. They may serve as a good example, however they require improvement by making sure it is less burdensome, complex, costly, time and resource demanding procedure, not limited to intra-group transfers,

included transfers to processors and ensure there is a higher level of transparency regarding the additional requirements at national level.

However it must be recognized that the approval process requires a great deal of time, resources and money and for this reason many companies have not been in a position to make the necessary investment in BCRs and have had to opt for other tools to enable international data transfers. To improve the existing systems, among others, the Council should be building on the existing system of mutual recognition to introduce a procedure in which a single lead DPA would take sole responsibility for reviewing, commenting on, and approving a particular BCR. This DPA's approval would then automatically be recognised by all other DPAs without any further local formality before other DPAs, such as e.g. requests for translations into local language. Such an approach would substantially improve on the existing EU system, which can often result in waits of between 18 months and three years. It is important to ensure that all national regulations adopted pursuant to the Convention have included an appropriate legal basis for mutual recognition of BCRs.

BCRS can be promising mechanisms for international data transfers as they provide a flexible means for organisations to move the data they control across borders while also guaranteeing robust protection for such data. With modern computing services such as strategic outsourcing and cloud computing, data processors should be also covered by BCRs. As a result, transferring data to and from such processors may necessitate complex contractual arrangements. Adapting BCRs to accommodate the operational realities in which data processors handle data in today's Information Society, could be an interesting tool as long as mechanisms are put in place to avoid the complexity and considerable resources needed in the current BCR approval process. Otherwise, companies that do not have the experience with BCRs or the means to invest the time, resources and money associated with such a complex procedure, would be put at a competitive disadvantage.

Process of formation and approval of BCRs, in order to serve their purpose adequately, should be made simple and fast, as well as harmonized among signatories.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

Before TAE can consider further or comment on the proposed changes to the Committee's role further details and greater clarification would be needed as to what form such a

strengthened Committee might take and the role, powers and authority it might be given. Without such level of detail it is not possible at this time to support such a move outright.
It is however suggested that this review may be an opportunity to consider how industry and other key stakeholder may be able to further support and input to the consultative committee already in place. For example the role and work of the ENISA Permanent Stakeholder Group could perhaps be looked at as an example of how to gain input and facilitate dialogue with industry on the Convention given its important role in the overall data protection legal framework in the EU and around the world.

UK – MINISTRY OF JUSTICE

Annex A

United Kingdom response to the consultation on the modernisation of Convention 108

We are grateful for the opportunity to respond to the Council of Europe's consultation. We consider the consultation to be a useful step in gathering evidence on the likely impact of challenges to the protection of personal data posed by globalisation and emergent technologies. It provides a helpful opportunity to review the effectiveness of data protection safeguards for citizens and consider whether they need to be updated or improved.

The Consultative Committee may wish to consider how the aim of a revised Convention will sit with the current review of the EU Data Protection Directive. It may be helpful to discuss the interaction between the Convention and the Directive and consider whether any issues may arise as a result of their concurrent revision.

Call for Evidence on the data protection legislative framework

The Consultative Committee may wish to note the UK launched a Call for Evidence on the UK data protection legislative framework on 6 July 2010, which closed on 6 October 2010. The Call for Evidence invited individuals, private organisations and public authorities to provide evidence on the current legislative framework on data protection, and in particular, how well it addresses certain specific or technical matters, how the current legislation is working and how it could be improved. Some of this subject matter directly corresponds to areas of the Bureau's consultation.

Over 160 written responses were received in response to the Call for Evidence from a range of interested parties, including central and local government, law enforcement authorities, trade unions, retailers, finance, technology and telecom companies, utility companies, small and medium enterprises, health organisations, legal organisations and information rights experts along with members of the public, civil society associations and consumer groups.

Our response to this consultation was published on 28 January 2011 (European Data Protection Day) and a copy of it was sent to the Bureau. The response is available online at: www.justice.gov.uk/consultations/docs/dpa-call-evidence-response-paper-28-01-11a.pdf

The UK also carried out a Post-Implementation Review (PIR) of the UK's DPA to assess the costs and benefits it has brought. This is available at: www.justice.gov.uk/consultations/docs/dpa-post-implement-review.pdf

These documents may be helpful to the Committee when considering any revision of the current Convention.

Comments on the consultation paper

Object and Scope of the Convention, Definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

We support the technologically neutral approach taken in this Convention and this is an important factor in its endurance for the last thirty years. The principles of Convention 108 remain sound and can be applied to any given situation. A more detailed approach would require constant updates to attempt to keep pace with technological advances – something which may prove difficult. The Consultative Committee has produced recommendations and guidance in response to specific issues and we believe that this approach should continue.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

We support the retention of the Convention's comprehensive approach, but recognise that the specific needs of law enforcement authorities need to be catered for to deal with the very different nature of law enforcement work from that in other sectors. We note the Consultative Committee's intention to consider whether related recommendations, such as Recommendation No. R(87) 15 of 17 September 1987 regulating the use of personal data in the police sector, should be revised.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

In principle, we would support the introduction of an exception for data processed in the course of a purely personal or household activity. This exception exists in the current EU legislation and would remove the inconsistency which exists between the Convention and EU law. However the question of what is included in domestic processing is complicated by the use of the internet, in particular blogs and social networking. We believe this is an area where further examination may be required.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

We would support in principle the introduction and further development of definitions, where they are consistent with those of the EU Data Protection Directive. We welcome the Council of Europe's initiative in attempting to reconcile the differences between existing EU legislation and the Council of Europe Convention – particularly where they increase safeguards for data subjects. There is a potential risk that if the Council of Europe were to adopt different definitions from those in EU legislation or new definitions, this would cause confusion for data controllers.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

The Convention already requires that personal data undergoing automatic processing shall be "adequate, relevant and not excessive" and therefore data controllers are already required to observe general principles of data minimisation and proportionality. If new ideas are to be introduced into the Convention then we would wish to understand fully the desired results and ensure that we were not creating disproportionate burdens for businesses, particularly small and medium sized ones, or creating confusion for individuals. Any burdens to businesses and other data controllers created by new proposals should of course be minimised and be proportionate to the actual benefits delivered to individuals by increased safeguards for more transparent processing. We recognise the financial and resource constraints within the Council of Europe in undertaking a thorough impact assessment of emerging proposals. If the Council of Europe is not in a position to undertake an assessment then we would encourage the Consultative Committee to take into account the work being done by the European Commission to assess the costs and benefits of their proposals in the review of the EU Data Protection Directive.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

We do not believe that consent is always a necessary condition for the processing of personal data to be fair, lawful and proportionate. The recent Council of Europe Recommendation on Profiling recognised this and included conditions similar to those which can be found in the Data Protection Directive such as "necessary for the performance of a contract to which the data subject is a party". Similarly, consent from those engaged in criminal activity is of course unlikely to be readily forthcoming as a basis for allowing the processing of their personal data. If the Convention is to be more detailed on this point, then it should acknowledge that consent is not the sole condition for fair and lawful processing.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

We welcome the opportunity to make the Convention's rules around legitimate processing consistent with those of the EU Directive.

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

The Convention provides, like the Data Protection Directive, that data may "not be used in a way incompatible with those [specified and legitimate] purposes". If a data controller uses personal data in a way which is incompatible with the original purpose for which it was collected then he is likely to be in breach of the principles. In our view the legislation is clear on this point.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its

processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

We are concerned that the unintended effect of extending the categories of sensitive personal data would be that some existing 'routine' processing would unnecessarily become subject to higher safeguards. The Consultative Committee may wish to consider whether the sensitivity of the data should be linked to its use rather than simply extending the current list of categories. For example, a photograph could be biometric data but there is a huge difference between a photograph of an individual on their library card and a photograph of the individual leaving a Drug Rehabilitation Centre. Many respondents to our Call for Evidence had views on this matter, which can be found from paragraph 12 onwards in the Government's response to the Call for Evidence.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

Specific obligations would provide greater clarity for data controllers, but we would also want to be clear about their potential impact on businesses as well as any financial and administrative burdens that may be involved. At a practical level, a consistent approach to the protection of children may be difficult to achieve because of the different definitions of childhood and adulthood across Council of Europe Member States.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

We would wish to establish how effective breach notifications have been in other jurisdictions, whether such notifications have delivered real value for citizens and whether as a result disproportionate costs have been imposed on businesses.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

We would wish to explore the introduction and greater use of accountability mechanisms further to assess what additional benefits they might deliver.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

We support the concept of 'Privacy by Design'. We believe that appropriate data protection safeguards should be built into the design of any new data processing operation rather than included as an expensive afterthought. We would be interested to know in more detail how this might be incorporated into a revised Convention 108.

Rights-Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

We would support the right of access covering the logic of the processing in the case of automated decision taking, as this would make a revised Convention consistent with Article 12a of the EU Data Protection Directive.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

The Consultative Committee may wish to consider whether the right of opposition should be closely aligned with the EU Data Protection Directive. Under Article 14 of the Directive the right to object (or right to opposition) is restricted to the conditions set out in Article 7(e) and 7(f) of the Directive. Therefore the data subject does not have the right to object to the processing of his personal data where the data controller is carrying out the processing, fairly and lawfully, in the vital interests of the data subject.

To some extent, the right to oblivion is already provided for in the Convention. Data controllers have an obligation to keep data only as long as necessary for the purposes for which the data has been collected and data subjects have a right to have data deleted or withdraw their consent. We are concerned that further development of the right to oblivion may involve costs and practical implications which need further consideration. Such a right could, if not limited in scope, seriously impede future historical research. It could also risk impeding delivery of services such as medical care, where knowledge of previous medical conditions and how they were managed can affect subsequent diagnoses and treatment.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

We believe that data controllers must take all reasonable steps to guarantee the security of their systems from unauthorised access to, and loss or disclosure of, personal data. We do not believe that there should be an absolute right to guarantee the confidentiality of individuals using information systems. For example, employers should be able to monitor their employees' use of their systems legitimately for the use of inappropriate websites, official time spent on personal web surfing and inappropriate uses of business email. Information service providers also use information from communication technologies for monitoring spam.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

We consider that such a right could become too broad and that there are many situations in which the use of geo-location data can be extremely valuable – for example, in locating missing persons.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

We do not believe that there should be an absolute right to remain anonymous when using information and communication technologies, as there are many situations where these should be legitimately monitored. Some information systems play an important role in prevention and detection of crime, for example, the UK's Child Exploitation Online Protection centre (CEOP) works with service providers to prevent the exploitation and abuse of children.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

This question is addressed to some extent in the EU Data Protection Directive, which provides that Member States are able to provide exemptions for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. We believe that this is sufficient.

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

We support the examination of alternative dispute resolution mechanisms and are keen to promote their use. The UK believes the public should be encouraged to resolve their issues out of court without recourse to public funds, using simpler, quicker, more informal remedies where they are appropriate. We are concerned about class actions being introduced in a revised Convention because of the potential resource implications for the justice system and the risk that it could pave the way for a more litigious society. We consider that collective redress should only be available where there is genuine need, rather than as a general principle across the legal system.

Data protection applicable law

24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

We consider that a rule determining the applicable law to data processing (where it involves different jurisdictions) may be difficult to achieve. With the advent of cloud-computing and internet communication, it will not always be clear which jurisdictions are involved and even less clear which one should take priority. We would welcome consultation on any further thinking in this area, but it may be that case-by-case consideration is better than a general rule.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

We support in principle examining how to guarantee the independence of national data protection authorities. We also support the proposal to examine ways to improve the cooperation and coordination between data protection authorities.

26. Should their role and tasks be specified?
We support some clarification of the role of data protection authorities within the Additional Protocol to Convention 108 along the lines set out in the Data Protection Directive. However, there is a risk that it could become overly-prescriptive and potentially undermine their freedom of action.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.
We agree that in principle an adequate level of protection should be ensured.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?
We welcome revisiting the notion of "transborder data flows" of personal data, as described in proposal 28. The advent of Cloud Computing and the exponential growth in the use of the Internet has changed the whole dynamic. We believe that increased attention should be paid to the competence and adequacy of the body handling the data and not just where the data is held. It may be helpful to consider the Madrid Declaration as a starting point for any revisions in this area.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?
We believe that data protection rules should be based on the type of processing, rather than the sector in which it is done. With some private companies now providing public services, for example, private medical services, it is often difficult to distinguish between the two. We do believe, as outlined above, that specific rules are needed in the police and judicial cooperation sector to cater for the specific type of processing that they do.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?
We would support examining ways to clarify the Committee's role and its powers.

Matters not raised in the Consultation

The UK believes that the Convention should continue to respect the different constitutions and legal systems of the Council of Europe Member States. For example, some countries' laws are codified, whereas others rely on Common law. We encourage the Consultative Committee to take this into account during the modernisation of Convention 108 and we look forward to further consultation.

UKRAINE – DATA PROTECTION AUTHORITY

The State Service of Ukraine on personal data protection head authority has a profound respect for you.

The State Service of Ukraine on personal data protection was established as a Supervisory authority in the scope of data protection on implementing the Act of Ukraine "On Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention 108; was ratificated by Ukraine: 06/07/2010; entered into force for Ukraine: 01/01/2011) and the Additional Protocol CETS 181, 2001; Convention for the Protection of Human Rights and Fundamental Freedoms; Directive 95/46; The Personal Data Protection Act of Ukraine, dated 01/06/2010 (entered into force on 01/01/2011).

However, the above mentioned information does not mean that there was no data protection legislation in Ukraine before December, 2010. Data protection was being regulated by the general Acts of Ukraine and of course by the Constitution of Ukraine during all this time.

The State Service of Ukraine on personal data protection has studies the entire question presented by the committee, as far as it is absolutely interested in all aspects and problems that were raised at the Conference. Today, however, it is still quite difficult for Ukraine to actually provide all the answers. Despite the great work being done and the dedication of the newly created The State Service of Ukraine on personal data protection, a short practice in the data protection scope does not let us to give the answers on all matters.

1. Convention 108 is the greatest achievement of the expert committee of the Council of Europe in the data protection scope. The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection"). The personal data undergoing processing shall be lodged to the certain demands, it shall be: obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. Concerning the fast-moving development in all the fields of our life, we need new improvements and modernization every day. That is why Convention 108 needs new text to be prepared, even though it is the first legally binding international instrument adopted in the field of data protection which is still in force nowadays.

2. Analyzing the differences in definitions of the "right to data protection" and "privacy", it is possible to conclude that nowadays Ukraine works considering the aspects of data protection. However, Ukraine agrees to agitate the "privacy" aspect.

3. In Ukrainian legislation, the law enforcement is plainly required to be performed. In addition to this, some provision in this scope from the Convention 108 are implemented into the Personal Data Protection Act of Ukraine.

4.

5. In the Ukrainian legislation, the automatic processing aspect is regulated by separate article of the Personal Data Protection Act of Ukraine. Concerning the definition of the controller of the file – the Personal Data Protection Act of Ukraine does not allow to have several controllers for one file. However, Ukraine is ready to agitate this aspect.

6. In the Personal Data Protection Act of Ukraine, it is used the definition of “processor”.

7. Ukraine agrees with the Convention modernization by adding the new principles, such as the proportionality principle and the data minimisation principle.

8. In our opinion, it is quite necessary to exercise the obligation to inform but at the same time it is necessary not to forget about the condition to make a fair and lawful processing.

9. Ukraine is ready to agitate these aspects.

10. In the Personal Data Protection Act of Ukraine, it is exactly governed that there is just one purpose of the data collection.

11. At the international stage it is very important to analyze and to represent the sensitive data categories.

12. Security concerns are important for everybody and always. Therefore, if it is a question of the creation such groups it is obligatory to attention to all social groups, not just to children. However, at first a great analytical work is needed to be made and completed, so experts will be able to point out the specialized social groups.

13. Yes, the notification of security should also include a right for data subjects to be informed of data security breaches.

14. Yes, the special rules on data traffic and data localisation are needed.

15. Ukraine agrees with the fact that accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules should be introduced.

16. According to the Ukrainian legislation, the principle of privacy by design is optional.

17. Yes, the right of access should also cover access to the logic of the data processing.

18. We agree with the fact that the articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

19. Yes, there should be a right to guarantee the confidentiality and integrity of information systems.

20. In our opinion, that a right “not to be tracked” (RFID tags) should be introduced. In our opinion, this idea has the right to life because of its real social need.

21. In our view, not everybody has a right to remain anonymous when using information and communication technologies, just in some cases. There has to be created a list of special circumstances.

22. In the reason of the rapid development of innovative technologies in the world, The State Service of Ukraine on personal data protection clearly agrees with the need of standards and requirements which provides Web.2.0.

23. .

24. In our opinion, a rule determining the applicable law to the data processing has to be considered.

25. The guarantee of the data protection authorities' independence has to be implemented by the national legislation. The international cooperation between national data protection authorities will work out if every country will be participating in different international events.

26. Yes, the data protection authorities' role and tasks have to be specified. In addition to this, we would like to inform you that in the Personal Data Protection Act of Ukraine they are also specified.

27. Ukraine agrees that adequate level of protection must be ensured. Ukraine has also ratificated the additional protocol to the Convention 108 (CETS 181, 2001).

28. Yes, we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders. In addition to that, we agree that it will be useful to establish internationally agreed minimum rules to ensure cross-border privacy.

29. In our view, there should be different rules for the public and private sector, in particular as regards the private sector there more use should be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules.

30. All efforts of the committee should be sent for the new standards accommodation.

Today the State Service of Ukraine on personal data protection official website and other electronic contacts are still being developed. However, in the nearest future we will get it. By today we are using a link on the Ministry of Justice of Ukraine website, which is:
http://www.minjust.gov.ua/0/str_minkoord_zpd

UKRAINE – MINISTRY OF JUSTICE

Object and Scope of the Convention, Definitions		
1.	Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?	Since 1981 Convention 108 was regarded to be a unique legal instrument in how it supports the exercise of rules for personal data protection. Its principles are to be a good standard for personal data protection in CoE countries. However, the main task for Convention 108 is to be valid in the face of new challenges, including globalisation, the ongoing march of technological capability and the changing ways that personal data is used. Although the flexibility of Convention 108 somehow helps it to remain current, its effectiveness is undermined by the complexity of the cultural and national differences across which it must operate. At that it modernization should be considered as an essential step forward for further development and enhancing data protection principles and standards.
2.	Should Convention 108 give a definition of the **right to data protection** and **privacy**?	Nowadays the link between the concept of personal data and real privacy risks is unclear. The privacy of individuals is affected by a number of intersecting drivers, including the need to process personal information for social and economic reasons, technological developments and trends such as the popularity of the Internet and globalisation. Privacy is recognised as a fundamental human right by various legal instruments, including the Universal Declaration of Human Rights (UN, 1948) and the European Convention on Human Rights (ECHR, Council of Europe, 1950). Privacy regulations aimed at governing how personal data is processed were introduced in the 1970s and 1980s, and the European Data Protection Directive came into force in 1995. Considering the issue that many of subject are requesting clarification on rights to data protection and privacy the great necessity exist for clear understanding as well as definition of this terms. In our position it will help better understanding of this issues and avoid misleading in it.

3.	Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?	All of individuals at any time will stay on the position to reject any intrusion to their privacy. But current issue is a double-edged weapon, as we should consider it both at the position of individual as well as take into account the position of competent authorities. That`s why we should find the golden mean on it and this issue is to be clearly stated in the Convention provisions. It is highly essential to clarify the possible situation when such an intrusion shall be legitimate and provide the way to protect individual and private interests.
4.	Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely **personal or household activity.** Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?	For today we do stay on the position to put this issue as it is. Considering that in the context of Web 2.0. all the information and data posted is provided under the agreement of individual introducing it, so again the emergent issue just the protection of such data from illegal use.
5.	The definition of **automatic processing** does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list? The definition of the **controller of the file** should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?	Current Ukrainian legislation contains the provision of collection within the definition of automatic processing. But in any case it is clear that some CoE countries may face the problem of collection determination within their national legislation and it would be much more easier for them to pass the amendments and supplements if the international standard (Convention 108) will contain such a requirement or at least such a countries may directly reference to it. As to review the controller definition in order to avoid misunderstandings with a few controllers it is possible to divide it on two definitions: controller (person which obtained the right for processing data) and processor (person empowered to process such data). And in our opinion it will simplify the understanding and using of such definitions.
6.	New definitions may be necessary, such as for the **processor** or the **manufacturer of technical equipment**.	See point 5 as well it is the same for manufacturer of technical equipment.
Protection principles		
7.	New principles could be added to the Convention, such as the **proportionality** principle, which should apply to all	The European Convention for the Protection of Human Rights and Fundamental Freedoms provides the proportionality

	operations carried out on the data. Such a principle is also linked to the **data minimization principle** which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.	principle with a special status as any derogation of the right to privacy is only permissible subject to a number of conditions, including its necessity in a democratic society (Article 8 of the Convention), which implies that such derogations should be kept to the strict minimum required to achieve the envisaged legitimate objective. Thus, it makes sense to harmonize these Conventions.
8.	Should the question of **consent** be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?	In our view there is no need to separate the principle of transparency and obligation to inform and fair and lawful processing. All these requirements should operate in conjunction that will provide and confirm the real legitimacy of the process.
9.	Should the **legitimate processing** be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?	Sure it should. First of all of the necessity to harmonize the international standards, as it simplify the conduction of assessments in the current sphere. And for sure it shall contain at least a minimum binding list of legal grounds and should not be exclusive so that the country could use it as a basis and in case of necessity to supplement it in the view of national requirements and legal traditions.
10.	Convention 108 does not expressly mention **compatibility in relation to purpose**. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.	At least the general principle should be covered by Convention 108 leaving the comprehensive procedures for the countries.
11.	**Special categories of data** which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?	All the data having impact on person`s privacy should be considered as a sensitive data. At that it is highly important to provide the detailed regime for it as well the detailed procedure for its processing.
12.	A specific protection could also be applied to certain categories of data subjects. In particular, **children** may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?	Protection is essential all the time and for all of us. In this issue we should not stand just on protection of children, as it is important to protect most vulnerable groups in society. But at the same time the great analysis is needed to make a clarify which essential minimum of special protection should be provided and which groups such a special

		protection will cover.
13.	Article 7 of the Convention addresses **security** in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of **data security breaches**?	It really sound idea as in practice it will aware the data subject on such a breach and will make it ready to protect its privacy and legitimate interests.
14.	There are special risks arising from the use of **traffic and localisation data** (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?	Sure, the special rules on data traffic and data localisation are needed, but here it is a necessity to involve the technical protection experts for clarification and advising the better ways on solving this issue.
15.	Should **accountability** mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?	Yes, as it often unclear where responsibility lies and who is accountable, especially in situations where a person's personal data can impact upon the privacy of others as well the controllers should be held accountable for their actions.
16.	Should the principle of **privacy by design**, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?	Sure it should, in any case the Convention 108 should cover as much general principles as possible.
Rights – Obligations		
17.	The **right of access** should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the **logic** of the processing?	Yes, the right of access should also cover access to the logic of the data processing.
18.	The **right of opposition** is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.	It quite sound idea but it should need the more detailed discussion and clarification.
19.	Should there be a right to guarantee the confidentiality and integrity of information	Yes

	systems?	
20.	Should a right 'not to be tracked' (RFID tags) be introduced?	Yes
21.	Should everyone have a right to remain anonymous when using information and communication technologies?	In a view of modern tendencies for transparency and rejecting anonymity it will be quite difficult to resolve this issue and come to a golden mean. But as a proposal may be considered an exclusive list of categories of subject, for example competent authorities, which may use such an anonymity. But it rather stays as an emerging issue.
22.	Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?	Somehow it should, but still it is too difficult to find such a balance. In any case the Convention 108 may stay on the position of reasonable legitimacy.
Sanctions and Remedies		
23.	Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?	Sure it should, in any case the Convention 108 should cover as much general principles as possible.
Data protection applicable law		
24.	Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?	The current practice for international cooperation of competent authorities shows that they consider using the existing national legislation by means of concluding separate agreements defining the applicable measures. But the general principle should be stated in the Convention.
Data Protection Authorities		
25.	How to guarantee their independence and ensure an international cooperation between national authorities?	As for the previous points the Convention should cover the general issue for independence but it still remains for the country to define on the national level the procedure and principles of international cooperation within the data protection area.
26.	Should their role and tasks be specified?	Yes, as much as possible and such a list should not be exclusive.
Transborder data flows		
27.	The aim of Convention 108 was to	It is a quite strong position and for sure

	reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.	countries bear responsibility for an adequate protection and as well the adequate assessment of such protection by means of specific requirements.
28.	Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?	Yes, but its content is essential to be set for a tour de table with open discussion during Working Party.
29.	Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?	Yes, again standing on the issue of data subject interests' protection.
Role of the consultative committee		
30.	Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?	We suppose to include the recommendation function and to combine the list of international experts who can be addressed for consultation or providing assistance in drafting legislation etc.

UNITED KINGDOM - INFORMATION COMMISSIONER'S OFFICE

Introduction

The Information Commissioner for the United Kingdom (ICUK) has responsibility for promoting and enforcing the UK Data Protection Act 1998 (DPA) and the UK Freedom of Information Act 2000. The Information Commissioner is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICUK does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The ICUK's response to this consultation is primarily based on the practical experience he has gained in regulating compliance with United Kingdom data protection law.

The ICUK agrees with the Council's assertion that the fundamental legal standards contained in Convention 108 remain valid. In particular, it is useful that the Council have highlighted that Convention 108 has a broader international application than European states. The ICUK also considers it particularly useful that the Council of Europe has published their position paper on modernising Convention 108 at the same time as other international data protection legal frameworks and standards initiatives are being consulted upon.

In the ICUK's opinion, an effective data protection framework must:

- be clear in its scope, particularly in the context of new forms of individual identification;
- protect the rights and freedoms of individuals whilst permitting the free flow of data;
- place clear responsibility and accountability on those processing personal data, throughout the information life cycle;
- ensure obligations for those processing personal data are focused on processing that poses genuine risk to individuals or society; rather than focusing on particular categories of data; and
- give individuals clear, effective rights and simple, cost-effective means of exercising them.

The ICUK hopes that this consultation exercise will eventually result in the development of data protection framework that has these features.

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

The ICUK would support continuing the drafting any modernised data protection framework in a technologically neutral way. This effectively provides a "future proofing" for any modernised Convention that can remain relevant even as technology progresses. To start to detail the type of technologies the standards might apply to in the future is to rely on the foresight of those drafting the Convention. Ten or even five years ago we could not have foreseen the impact of technologies such as biometrics, social networking, targeted behavioural advertising, near field communications or cloud computing. Writing a legal text that could ensure that comparable future developments are adequately covered is therefore an impossible task.

This is not to say that the ICUK cannot see a need to provide greater detail in the drafting of a modernised Convention. But this should focus on providing greater clarity around the fundamental concepts of data protection, rather than detailing the type of technologies that the Convention should apply to. A modernised Convention 108 should be a "living instrument" that can be applied

to technology as it advances, rather than an instrument that has a progressively narrower application as new technologies come to the fore and current technologies become obsolete.

Any modernised legislative framework should continue to apply to both direct and indirect forms of identification. However, there is evidence of considerable uncertainty in the practical application of the current law to information that identifies people indirectly. A modernised Convention should open the way for a more realistic treatment of this sort of information. For example, it might require the security principle to apply to all forms of personal data, but acknowledge the practical difficulty involved in obtaining consent for the processing of, or the granting of subject access to, some information that indentifies individuals indirectly. A simple 'all or nothing' approach to data protection requirements no longer suffices, given the variety of information that can now fall within the definition of personal data. The requirements should be more clearly linked to the risk to individual privacy.

2. Should Convention 108 give a definition of the right to data protection and privacy?

The right to privacy is enshrined in several other Conventions and international agreements. Data protection applies the right to privacy to personal data, drawing out specific obligations on data controllers and specific rights for data subjects, including subject access, rectification and destruction and the right to object to certain processing.

While the ICUK does not see the need to provide another definition of the right to privacy or a right to data protection, he sees the value in being explicit about the strong links between Convention 108 and the rights enshrined in the European Convention on Human Rights, in particular those Article 8 rights to a private and family life, home and correspondence.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

The ICUK considers it vital that any modernised Convention retain the comprehensive coverage of scope. While the ICUK appreciates that other instruments, such as the EU Data Protection Directive, have explicitly excluded law enforcement and judicial authorities from their scope, the European Commission has now stated that it is considering extending EU data protection rules to the areas of police and judicial cooperation in criminal matters[306]. UK data protection law already applies to these areas, albeit with appropriate exemptions which allow police and judicial services to operate effectively.

The current debate on the future of data protection is to broaden the scope to cover these areas, to adopt the comprehensive approach that has been a cornerstone of Convention 108 since its adoption in 1981. The ICUK supports this approach and his experience is that high standards of personal data protection are neither incompatible with, nor an impediment to, effective law enforcement and judicial services. It would be unfortunate if a modernised Convention abandoned the comprehensive approach.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

[306] See Chapter 2.3 of "A comprehensive approach on personal data protection in the European Union", a Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 4 November 2010

Other instruments exclude from their scope data processed by a natural person in the course of purely personal or household activity, such as the EU Data Protection Directive. The ICUK supports this notion.

However, the ICUK considers it vital that a better understanding is needed of what comes within the scope of purely personal or household activity. This is becoming an acute practical problem given private individuals' capacity to process personal data on the internet and to make it widely available to other individuals, for example, through social networking services. There are also questions about how far such an exclusion can be applied to the activities of private individuals on the internet. There are also significant practical consequences for data protection authorities in terms of the extent to which any modernised Convention may require them to regulate private individuals' online behaviour.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The ICUK considers it vital that the collection of data is included in the definition of automatic processing, or at the very least data which is intended to be processed by automatic means is brought within the scope of any modernised Convention. This would bring the Convention in line with other national and international data protection instruments.

The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

There can be a lack of clarity and certainty in determining which organisation is the "controller of the file" in relationships between organisations that process personal information. The complexity of modern business relationships means that there are endless possibilities and the question of who takes ultimate responsibility for ensuring that personal information is processed in accordance with the law is often opaque. This is not helped by very general definition as to what constitutes a "controller". The ICUK would support reviewing this definition.

In terms of whether there should be several criteria listed, and whether these criteria should be cumulative, the ICUK would again say that the complexity of modern business relationships could not have been foreseen 10 years ago. Rather than list criteria as to what constitutes a "controller", the ICUK would see value in providing a better description as to what activities a controller of the file would undertake.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

With regard to the ICUK's experience of definitions in the EU Data Protection Directive, it is clear that a simple distinction between a controller and a processor no longer reflects the complicated relationships that exist between organisations processing personal data. The definitions of "controller" and "processor" in Article 2 of the EU Data Protection Directive assume that there is always a clear distinction between those who determine the means and purpose of the processing and those who process on behalf of the controller. The definitions assume that a processor is an essentially passive entity, acting on behalf of a controller, with no independent influence over the way the processing takes place. This does not reflect the reality of current business practice where an organisation that at first sight appears to be a processor – typically a sub-contractor – may exercise considerable influence over the way the processing takes place and may, in many respects, act as a controller. This situation is made all the more difficult because subcontractors

may outsource certain aspects of their work to other subcontractors. This can make it difficult to establish responsibility, for example, in enforcement cases.

An explicit accountability principle might help deal with controller-processor relationships that are difficult to define.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

The ICUK would support building proportionality more explicitly into any modernised Convention.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

The relationship between these two aspects of fairness can be confusing. An emphasis on consent rather than transparency, or vice versa, can give a very different complexion to data protection regimes. It can confuse individuals and can cause great practical uncertainty for controllers. A new legislative framework should give a clearer indication of when consent is needed to legitimise the processing of personal data, and when it is sufficient for individuals to be merely aware that the processing is taking place. Consent should only be used to legitimise processing where individuals have genuinely free choice.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

The ICUK has some doubt about the legal framework that involves the need to satisfy a condition to legitimise the processing of personal data, and an additional condition where sensitive personal data are involved. He believes that this can result in the artificial justification or restriction of otherwise unobjectionable processing and offers little meaningful protection to individuals. Indeed the predecessor to the current UK DPA, the Data Protection Act 1984, did not contain special provisions governing the processing of sensitive personal data. In practice this did not stand in the way of the proper protection of genuinely sensitive data, but provided more flexibility for business and the ICUK in the way this was delivered.

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

The ICUK would make two points here. The first is in relation to his approach to compatibility of purpose. The ICUK considers that much of the protection that is provided by the compatibility principle is provided by fairness and transparency about the purposes for which personal data are used. Both the EU DP Directive and the UK DPA make explicit reference to compatibility with "specified" purposes, which makes a strong link with transparency of processing operations. Often a breach of the compatibility principle is also a breach of the fairness principle.

The second point is that where the EU DP Directive and the UK DPA have a compatibility principle, both actually refer to further purposes not being incompatible with the specified purposes.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

The term 'biometric personal data' is perhaps misleading. Biometry involves capturing a piece of biological information, such as a measurement of a person's facial features, and using an algorithm to convert this into a biometric – put simply a set of numbers. A reader is then used to determine whether biological information presented to it on a subsequent occasion corresponds with the biometric already held in a database. This process is used to determine whether a person should be allowed to enter a building, for example. Therefore any new legislative framework needs to draw a distinction between the raw biological data from which a biometric is derived, and the biometric itself; the terms are sometimes used interchangeably.

The ICUK is not of the opinion that a physical or biological characteristic should necessarily be included within the definition of 'sensitive personal data'. Nor does he consider that the biometric itself should necessarily be considered 'sensitive'. This is because of the wide range of biometric systems in existence and their varying effect on individuals. The ICUK's view is that sensitivity arises from the overall nature of the processing operation, particularly its actual or potential effect on individuals, rather than just the nature of the information being processed.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

The application of data protection law to children raises a number of difficult issues for children, parents and those that process personal data about children. Some have suggested that in future data protection law could regulate the processing of children's data better, primarily by specifying an age at which childhood ends and adulthood begins, and by setting out specific requirements for the processing of data about children. However, we are sceptical as to what this would achieve in terms of the informational protection of children. This is because rules for defining a child vary across the world. In some countries there is a clear age limit, in others – such as the UK – there is no legal definition of a child. We do not anticipate a modernised Convention being able to harmonise this. The other problem is that different age groups of children, and indeed different individuals within those groups, can have very different levels of maturity and understanding. We envisage it being highly problematic to formulate a set of detailed data protection rules that are as applicable to a five year old as they are to a child in his or her teenage years, for example. The law should recognise that even relatively young children can understand simple low-risk propositions, for example, when they decide to provide their contact details when they sign up for an electronic newsletter.

We also note the formidable practical difficulties involved in setting up mechanisms for verifying a child's age or for obtaining parental consent; mechanisms that are relatively easy for a determined child to circumvent.

For these reasons we do not support the inclusion of detailed provisions that relate specifically to children. However, we think that the law should encourage initiatives such as industry codes of practice, setting out detailed rules for processing personal data about children in particular contexts – for example, marketing goods and services to specific age-groups.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

It should be a prerequisite that in revising any of the current obligations on controllers, and in introducing any new obligations, those obligations have a substantive effect on the protection of privacy, and reduction of risk to the individual. New measures should not be introduced that add to the burden on data controllers but do not significantly add to the protection of the privacy of the individual.

The ICUK considers that, in the right circumstances, breach notification can significantly enhance data protection. However, the introduction of a general breach notification requirement must have a sound evidential base that demonstrates it will have a significant impact on the protection of personal data, and must be framed in such a way as to avoid becoming merely a way of complying on paper, with no substantive effect on information privacy in practice.

An alternative might be to require controllers to have a breach notification policy in place.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

The ICUK would reiterate that it is his view that sensitivity arises from the overall nature of the processing operation, particularly its actual or potential effect on individuals, rather than just the nature of the information being processed.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

The Information Commissioner would like to see a new, general requirement of accountability introduced. This would reinforce the responsibility of controllers for ensuring that personal information is properly protected in practice by requiring them to:

- take appropriate and effective measures to implement data protection principles; and
- be able to demonstrate, on request, that such measures have been taken.

The requirement would not impose any additional burden on controllers that take their responsibilities seriously, but would emphasise, on the face of the Convention, that data controllers have to take concrete measures to deliver effective data protection in practice. It would, through the transparency element, also assist DP authorities in targeting their activities on areas of genuine DP risk.

An accountability requirement would have to be scalable to the size of the organisation concerned and the risks of the processing of personal data they perform, so as not to impose any further unwarranted obligations on controllers. Whilst a large multinational might be expected to have measures in place such as relevant policies and procedures, a data protection official, privacy impact assessments and training programmes, a small or medium enterprise would not necessarily be expected to do any more than be able to explain the steps it has taken to identify and address any risks its business poses to the privacy of personal information. Accountability already features in some DP regimes including the OECD privacy guidelines and the APEC privacy framework. Its introduction as a principle in the Convention would promote global harmonisation of DP

requirements and could contribute to reducing the administrative burden imposed by the current rules on international data transfers.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

The principle of privacy by design is implicit in the existing data protection principles - for example, the requirement that personal data shall not be excessive. However, an explicit privacy by design requirement would give a clear message to those designing, procuring and operating information systems that the processing of personal data must be done in the most privacy friendly way practicable.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

The ICUK would support this as it is already covered in the right of access provided in both the EU DP Directive and the UK DPA.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

The ICUK can see some situations where the "right to oblivion" could work well in practice, such as where an individual wishes to delete their record from a social network, but these situations are limited. It is essential that individuals understand the nature and extent of their rights, and that those rights are framed in a way that is not misleading to the individual. The "right to oblivion" suggests possibilities that may not actually be available to the individual, or that in some cases could work against their fundamental rights and freedoms. It could also be technologically difficult for this right to be delivered in practice in some circumstances, such as when the information has been made publicly available on the internet.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

The ICUK would question the value of making this a "right" for the individual, as opposed to the greater value in strengthening the provisions of the principle of data security. How would individuals assert this right? More clarity is needed on the exact nature of this provision if it to be framed as a right to individuals.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

This right will need some thinking through. Tracking happens using more than just RFID tags and to produce a right based on one type of technology seems to run contrary to the aim of keeping the Convention technology neutral.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

There are three questions to ask in relation to the right to be anonymous. The first question is to whom the individual is anonymous. Is it their communications service provider, the websites that they visit, third parties engaged by the CSP or website, national authorities or other individuals with whom they may be communicating?

This leads to the second question. Where is providing this right technically possible? Traffic data has to be processed by the communications service provider for billing purposes. Websites need to use cookies in some circumstances to provide interactive services to the individual.

The final question is where is this right desirable? For example, does an individual have the right to remain anonymous when using information and communications technologies to harass other individuals, to disrupt emergency services or break the law? The UK Privacy and Electronic Communications regulations place an obligation on telecommunications service providers to allow individuals to withhold their number from the recipient when making a call. However, the telecommunications service provider may override this right, in so far as it appears to the provider in question to be necessary, to trace malicious or nuisance calls. The right does not exist at all where the call is made to emergency services.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

There are also significant practical consequences for data protection authorities in terms of the extent to which any new legislative framework may require them to regulate private individuals' online behaviour.

Connected to this, but of broader significance, is the need to balance a high standard of data protection against a strong upholding of the right to freedom of expression. In an age of online blogging, where should the line be drawn in any future Convention?

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

The ICUK would support both of these measures. In particular, the ICUK considers giving more scope to alternative dispute resolution to be of paramount importance. But there is a broader point. Organisations should also be encouraged to 'self-regulate' as far as possible, for example, by adopting sectoral codes or applying recognised standards for collecting and handling personal information. The ICUK has no doubt that effective self-regulation by organisations (perhaps backed up by some form of accreditation), and self-protection by well informed individuals, are important elements of a modern data protection regime. A future framework should acknowledge and promote this.

With complaints handling, data protection authorities need the freedom to set up procedures to suit their resources and the local conditions. For example, it would be helpful if a modernised Convention provided a clear basis for data protection authorities to approve other complaint handling mechanisms, so as to be able to work with other relevant regulators or industry groups who may be able to achieve better or more cost effective results for individuals. The Commissioner has significant doubts as to the sustainability of a state of affairs where data protection authorities are expected to deal with every complaint about every aspect of the processing of personal information – particularly at a time when resources are being cut back.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

Within the EU, data protection authorities are set up differently in the various member states and so are independent in different ways. In other countries, particularly those outside Europe who can now sign up to the Convention, the supervisory functions may be done by a separate authority or within an organisation. What is important is that the current Article 1(3) of the Additional Protocol (CETS 181, 2001) is extended to specify what is to be understood by independence.

For example, in Ireland the Commissioner is appointed by the government, but is independent in the exercise of his or her functions. In Canada, the Privacy Commissioner is an Officer of Parliament who reports directly to the House of Commons and the Senate. Both are considered independent supervisory authorities. In the UK, the ICUK considers the fact that his data protection work is funded by notification fees to be a crucial factor in his independence. This fee-based funding mechanism also ensures the ICUK has the necessary budget to fulfill his duties, which is particularly relevant in the current economic climate.

It might be helpful to update the additional protocol to specify that independence includes, for example, sufficient funding to carry out duties and obligations; independence in the exercise of functions; the freedom to set priorities and strategy; the head of the authority appointed by and reporting to the national Parliament or its equivalent.

With regard to international co-operation between authorities, the current provisions in Article 13(3)(b) of the Convention and Article 1(5) of the Additional Protocol are a barrier to authorities co-operating. This is because the provisions prevent the exchange of the personal data related to the issue that the authorities are co-operating to resolve. In the experience of the ICUK, most complaints that need co-operation with another authority to resolve involve exchanging the relevant personal data of the complainant. Without this information authorities cannot carry out the necessary checks and investigations to resolve the complaint.

The ICUK strongly recommends adding to or clarifying the articles mentioned above to ensure that supervisory authorities are able to co-operate fully, exchanging all necessary information including personal data, to ensure effective protection for individuals. To the ICUK's knowledge, all supervisory authorities have appropriate safeguards in their national law with regard to disclosures of information by staff. For example, in the UK it is a criminal offence for any ICO member of staff to disclose information relating to an identifiable individual obtained in the course of their duties to anyone outside the authority[307].

26. Should their role and tasks be specified?

The current data protection framework has resulted in many differences in the roles, remits and powers of national data protection authorities. What should the mixture of education, 'policing', complaints handling and policy activity? Whilst some degree of diversity between national data protection authorities is healthy and perhaps inevitable, the Commissioner recognises that the current situation can be confusing for data controllers that operate internationally – are they dealing with a tough policeman or a helpful educator in any particular country? It would be helpful if a future legal framework could do more to clarify what features and characteristics a modern data protection authority should have. In particular, the Information Commissioner is of the opinion that the role of

[307] See section 59 of the DPA 98 for the details.

the national authority as educator must be maintained as an explicit part of any modernised Convention.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

This is one area that most needs to be amended to deal more realistically with current and future international dataflows. A modernised Convention should focus much more on risk assessment by the exporting data controller and should be clearer about data controllers' responsibility, wherever they choose to process personal data. The ICUK has doubts about a concept of adequacy based substantially on the nature of the law in place in a particular territory. Adequacy should be assessed more in relation to the specific circumstances of the transfer and less on the adequacy or otherwise of the law of the country the recipient is established in. Clearly the law in place in the recipient country is a factor, but it should not be the principal means of determining the adequacy of a transfer.

The current system for determining whether a third country has an adequate level of data protection is slow and cumbersome, and only a few countries have to date achieved an adequacy finding. This system may still be part of the solution in the future legal framework, but it needs to be a quicker and simpler process. The Convention should also reaffirm the position that the test is adequacy, not equivalence. However, findings of adequacy should not be the only option; there need to be more flexible solutions for recognising the adequacy of organisations or sectors in non-adequate countries. For example, those signed up to recognised industry codes of practice, or self-regulatory systems. There is also a link here to the points made on accountability, with the possibility that properly accountable organisations in third countries could be deemed adequate for the transfer of personal data.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

The ICUK favours a system under which methods of transfers, not transfers by individual businesses, are approved. Any approval of a method of transfer (such as contractual clauses, BCR) should be underpinned by a legally established system of mutual recognition.

In terms of whether the public and private sectors have differing rules, this becomes ever more difficult in a world where the public sector increasingly engages the private sector to deliver services, and where public sector practice increasingly draws on private sector experience. The ICUK's experience suggests that having different methods to ensure adequacy is beneficial, but it should be left to the controller to determine which method they consider to be most appropriate for determining adequacy.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

While the ICUK considers this to be generally beneficial, the role of the consultative Committee must not place additional burdens on Member States and/or national authorities. There are several supra-national bodies in existence that may set standards, resolve disputes and monitor functions, and the European Commission's data protection strategy points to reforming the Article 29 Working Party to perform some of these roles.

Any revised role of the consultative committee must avoid duplication of effort or contradictory standards.

U.S. FEDERAL TRADE COMMISSION

U.S. Federal Trade Commission Staff Comments to the Council of Europe's Consultative Committee on the Modernization of Convention 108[1]

March 9, 2011

I. Introduction

United States Federal Trade Commission (FTC) staff submits the following comments to the Council of Europe's Consultative Committee in response to its request for comments on modernizing the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its 2001 Protocol regarding supervisory authorities and transborder data flows ("Convention 108").

The FTC staff commends the Consultative Committee on undertaking this review, and for raising many critical questions in contemplating this modernization, as set forth in the Consultative Committee's consultation paper requesting comments.[2] The consultation paper raises a broad array of very complex questions, and given time constraints we cannot address all the relevant ones here. Moreover, we are mindful that we submit our comments as outside observers; the United States is of course not a party to Convention 108. Instead, we offer at this time comments on a few of the key issues raised, and some background on our own consultation process on many similar issues.

As the Consultative Committee is aware, the European Commission (EC) is also considering how to improve the privacy framework in the European Union (EU). The Organization for Economic Cooperation and Development (OECD) is also examining the 1980 OECD Privacy Guidelines, and as described below, the FTC has also undertaken a wide-ranging initiative to consider how the U.S. privacy framework might be improved. We believe there is great value in continuing the dialogue among the various bodies examining privacy frameworks. The FTC participates in the OECD committee examining the 1980 Privacy Guidelines, and has taken several opportunities to engage with the European Commission on its work developing an improved privacy framework in the EU.[3] We appreciated the opportunity for FTC staff and FTC Commissioner Julie Brill to meet with the Council of Europe's Deputy Secretary General Maud de Boer-Buquicchio last week, and we welcome further occasions to exchange views on these issues.

II. FTC Examination

For more than a year, the FTC has been re-examining the privacy framework now used in the United States. In December 2009, the FTC hosted the first of three roundtables to explore the privacy issues and challenges associated with 21st century technology and business practices.

---

[1] These comments represent the views of the staff of the Federal Trade Commission, and not necessarily the views of the Federal Trade Commission itself or any individual FTC commissioner.

[2] *Available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf.

[3] The FTC staff submitted comments to the European Commission (EC) in connection with the EC consultation. These comments, submitted on January 13, 2011, are *available at* http://www.ftc.gov/os/2011/01/111301dataprotectframework.pdf

We organized two additional roundtables in January and March of 2010. On December 1, 2010, FTC staff issued a 122-page preliminary report that builds on the themes that emerged at the three roundtables, and that proposes a framework capable of protecting the privacy interests of consumers while also permitting the use of consumer information to develop beneficial new products and services ("FTC Report").[4] We think you will find considerable material in the FTC Report that addresses the issues raised in your consultation process.

We also note that the U.S. Department of Commerce issued a paper on December 16, 2010, containing policy recommendations in the privacy area—*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[5] This paper is the result of a U.S. Department of Commerce public consultation initiative.

The FTC Report makes a number of recommendations, including the following: (a) companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices; (b) consumers should be presented with choice about collection and sharing of their data at the time and in the context in which they are making decisions about the collection or use of their data; and (c) information practices should be more transparent to consumers and consumers should be allowed reasonable access to the data companies maintain about them, particularly for non-consumer facing entities such as data brokers.

The FTC Report also suggests implementation of a "Do Not Track" mechanism for online behavioral advertising – likely a persistent setting on consumers' browsers – so consumers can choose whether to allow the companies to collect information about them as they browse the web.

The FTC Report requested comment on the proposals made; we received more than 400 comments, including some from foreign counterparts. We expect that FTC staff will issue another report later this year that takes into account the input received in these numerous comments.

III. Consultative Committee Consultation Paper

The Consultative Committee Consultation Paper raises a number of issues and questions in considering modernizing Convention 108. We take this opportunity to provide the Consultative Committee with input on several of the issues and questions raised in the Consultation Paper.

A. Consent.

The Consultation Paper asks:

---

[4] FTC Staff, *Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (2010) ("FTC Report"), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[5] *Available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf

Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

The FTC Report emphasizes that greater transparency is essential in an improved privacy framework. The FTC Report points out that many data practices are invisible to consumers, and therefore we encourage companies to implement a number of measures to make their data practices more transparent to consumers. [6] For example, one idea discussed in the FTC Report is the need to simplify consumer choice and to provide choice mechanisms in a prominent, relevant, and easily accessible place for consumers.[7]

Having said that, the FTC Report also suggests that for commonly accepted practices, choice should not be necessary; eliminating choices for practices obvious to consumers would make the choices for practices of greater concern more meaningful.[8] For example, consumers are aware that their information would be provided to the shipper to fulfill an online order—mandating choice for this use distracts consumers from the choices they need to make in other areas, for example disclosure of their information to third parties unrelated to order fulfillment. Thus, we encourage the Consultative Committee to consider the question of consent taking into account commonly accepted practices where consent may not be necessary.

B. Children.

The Consultation Paper raises the following points:

A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

We note that in the United States, a specialized statute governs children's online privacy. This statue, the Children's Online Privacy Protection Act (COPPA)[9] requires that the FTC issue and enforce a rule protecting children's online privacy. This Rule went into effect in April 2000.[10] We believe that there are unique issues relating to the online privacy of children, and formulating a specialized rule has been useful in this area.

The primary goal of the COPPA statute and Rule is to put parents in control over what information is collected from their children online. The Rule was designed to protect children

---

[6] "[C]onsumers are generally unaware of the number of online and offline entities that collect their data, the breadth of the data collected, and the extent to which data is shared with third parties that are often entirely unknown to consumers." FTC Report at 42.

[7] FTC Report at 52-69.

[8] FTC Report at 53-57.

[9] 15 U.S.C. §§ 6501-6506.

[10] 16 C.F.R. Part 312.

under age 13 while accounting for the dynamic nature of the Internet. The Rule applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. Businesses covered by the Rule must:

1. Post a clear and comprehensive privacy policy on their website describing their information practices for children's personal information;

2. Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information from children;

3. Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties;

4. Provide parents access to their child's personal information to review and/or have the information deleted;

5. Give parents the opportunity to prevent further use or online collection of a child's personal information;

6. Maintain the confidentiality, security, and integrity of information they collect from children.

In addition, the Rule prohibits operators from conditioning a child's participation in an online activity on the child's providing more information than is reasonably necessary to participate in that activity.

It has been nearly eleven years since the Rule went into effect. In light of the rapid-fire pace of technological developments in recent years, including an explosion in children's use of mobile devices and interactive gaming, the FTC accelerated its review of COPPA to make sure that it is still adequately protecting children's privacy. The review was earlier scheduled to take place in 2015, but the FTC accelerated this process and in March 2010, sought comments on revising the Rule.[11] In addition, in June 2010, the FTC hosted a public roundtable on issues relating to the Rule.[12] FTC staff is currently reviewing comments received from a broad range of stakeholders and is considering whether there is a need for any modifications to the Rule.

C. Data Security

The Consultation Paper asks:

---

[11] Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2010), *available at* http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf.

[12] http://www.ftc.gov/bcp/workshops/coppa/index.shtml.

Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

The FTC believes that data breach notification in appropriate circumstances is beneficial. In the United States, many of the individual states have passed breach notification laws and some also have imposed data security requirements on companies operating within their states. These laws have further increased public awareness of data security issues and related harms, as well as data security issues at specific companies. The FTC has been advocating for breach notification legislation at the federal level in order to extend notification nationwide. We note that one of the most important considerations in contemplating breach notification is determining the thresholds that would trigger the notification requirement. It may not be appropriate to require notification in all circumstances—certain factors should be taken into account, including the extent of the breach and the likelihood of injury. Requiring notification in every situation may distract consumers from those breaches that are of the greatest concern.

D. Accountability.

The Consultative Committee Consultation paper asks:

Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

We encourage the development of mechanisms that would enable companies to demonstrate compliance with laws, regulations, self-regulatory codes of conduct, or their own internal policies and procedures. As discussed in more detail in paragraph III.G, below, an effort to promote greater accountability in the privacy area, through the development of cross-border privacy rules, is underway within the Asia-Pacific region through the work of the Asia-Pacific Economic Cooperation (APEC) forum. Such an accountability mechanism holds great promise, both domestically, and in the area of cross-border data transfers, and we encourage dialogue within the international privacy community to consider how to develop additional mechanisms.

E. Privacy by Design.

The Consultative Committee Consultation paper asks:

Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

In the FTC Report, we recommend that companies adopt a "Privacy by Design" approach.[13] This would involve building privacy protections into everyday business practices. These protections would include providing reasonable security for personal information,

[13] FTC Report at 41.

collecting only the data necessary for a specific business purpose, and retaining data only for the period of time required to fulfill that purpose.

The FTC Report further notes that the implementation of "Privacy by Design" within industry can be scaled to each company's business operations.[14] This takes into account company differences, including size, amount of personal information collected, and type of personal information collected. We would encourage the Consultative Committee to consider the important concept of scalability in considering the issue of Privacy by Design.

F. Access. The Consultative Committee Consultation Paper asks:

> *The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?*

We are unclear on what is meant by the "access to the logic" of the processing of the data and would appreciate clarification on this point. Perhaps this refers to providing individuals with the company's reasoning with regard to certain decisions made impacting consumers. We note that in the United States, consumers have a right to be informed if certain companies take an action that has a negative impact on the consumer, if such action was based at least in part on information contained in the consumer's credit report. In such event, consumers would also have the right to obtain a copy of their credit report. An example of an action having a negative impact (the term used in U.S. law is "adverse action") includes the denial or cancellation of credit or insurance, or the denying of employment or promotion.[15] Consumers also have a right to obtain a credit score, generally for a small fee.[16] While credit reporting agencies are not required to reveal precisely how credit scores are calculated, the disclosure must include the range of possible credit scores in the scoring model and key factors that adversely affected the consumer's score.[17]

We note that the FTC Report proposes providing consumers with reasonable access to the data that companies maintain about them, particularly for companies that do not interact with consumers directly, such as data brokers. We are mindful, however, of the significant costs associated with access. Accordingly, we suggest that the extent of access should be proportional to both the sensitivity of the data and its intended use.[18]

The FTC Report raises a number of questions relating to access, and we specifically sought comment on these issues. Among the questions are: (a) whether companies should be able to charge a reasonable cost for certain types of access; (b) whether companies should be required to inform consumers of the identity of those with whom the company has shared data

---

[14] FTC Report at v.

[15] 15 U.S.C. 1681m(a).

[16] 15 U.S.C. 1681g(f).

[17] *Id.*

[18] FTC Report at 72-76.

about the consumer, as well as how they obtained the data; and (c) whether access to data should differ for consumer-facing and non-consumer-facing entities.

We would be interested in learning more about the Consultative Committee's rationale in determining that access rights should include the origin of the information that a company has about an individual—as noted above, that is one of the questions posed in the FTC Report.

G. Free Flow of Information.

The Consultative Committee Consultation Paper asks:

> *Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?*

We note that like the EU Data Protection Directive, the Additional Protocol to Convention 108 contains an "adequacy" provision. The "adequacy" approach focuses on the legal framework of the jurisdiction where the data recipient is located, and not on the data protection practices of the actual data recipient. As we have noted in our comments to the European Commission, significant shortcomings in the "adequacy" framework include the lack of clarity in the procedure and the cumbersome nature of the process. Research suggests that in the EU, "rules on data export and transfer to third countries are outmoded," and that "the tools providing for transfer to third countries are cumbersome."[19] The process appears if anything more complex for countries applying both the EU and the Convention 108 adequacy standards. This suggests that there may be value in reconsidering the Convention 108 "adequacy" requirement, and also in considering the impact of having data flow restrictions in two different regional legal instruments with overlapping signatories.

The FTC is currently involved in the privacy-related work of APEC, where efforts are underway to develop more workable mechanisms relating to the cross-border transfer of data.[20] In particular, we have been working on the development of the APEC cross-border privacy rules system. This is a reciprocal program governing cross-border information transfers among companies in the APEC region. Once the system is operational, we believe that it has tremendous potential to facilitate accountable and efficient data transfers within the APEC region. All stakeholders in such a system could benefit significantly—consumers because they are dealing with accountable organizations who have opted into an efficient privacy management system that includes effective complaint resolution procedures; companies because the system creates greater efficiency, uniformity and predictability with respect to their privacy and data security requirements; and privacy enforcement authorities such as the FTC, because an efficient self-regulatory system, coupled with effective backstop enforcement contingencies, improves the effectiveness of their privacy enforcement missions.

---

[19] See Review of the European Data Protection Directive, Rand Europe (2009) at 33-34, available at http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf

[20] See http://www.apec.org/en/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx.

With regard to internationally agreed-upon privacy rules, we believe that at this stage, the primary focus should be on the development of an appropriate procedural framework for considering how a global standard might be developed, based on input from all international regions and stakeholders, including those that are currently still in the process of rethinking, modernizing and establishing their regional privacy approaches.

FTC staff previously stressed the importance of such a process in its comments on the International Conference of Data Protection and Privacy Commissioner's *Joint Proposal for International Standards on the Protection Of Privacy With Regard to the Processing Of Personal Data*.[21] In our August 2010 comments on the *Joint Proposal*, which we prepared jointly with the Privacy Office of the U.S. Department of Homeland Security, we recommended that "all relevant stakeholders in the international privacy dialogue collaborate and develop a meaningful way to achieve broader input on the feasibility of an international data privacy standard."[22]

Data protection and privacy are highly complex and technical subjects in which there remain significant unresolved political and policy debates. Indeed, the United States, the European Commission, and the OECD are also in the process of reviewing their respective frameworks. We also point out that the United Nations' International Law Commission has commented that data protection is an area "in which State practice is not yet extensive or fully developed."[23]

U.S.

We commend the Consultative Committee on undertaking this review, and for raising many critical questions in contemplating this modernization, as set forth in the Consultative Committee's consultation paper requesting comments.[308] We recognize that Convention 108 has served as the backbone of international law in over 40 European countries and applaud the Council's efforts to reach out to non-European states as it seeks broader application through modernization. The paper raises a broad array of very complex questions, and given time constraints we cannot address all the relevant ones here. Moreover, we are mindful that we submit our comments as outside observers; the United States is of course not a party to Convention 108. Instead, we offer at this time only a general comment on the scope of the possible revision as it relates to our role in protecting data privacy in various areas of law enforcement and security, which increasingly interrelates to those of our European partners.

The Consultation paper states:

Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Given the special nature of the role of the public sector in law enforcement and security, this question must be answered either at the outset or the conclusion of the revision. Answers to other issues raised in the Consultation paper, such as legitimate processing, proportionality, consent, breach notification, accountability, special categories of data, right of access and right of opposition, will need to take into account the practical application of law enforcement and security if they are to apply in this area.

We are most concerned with the interplay between the application of the Convention to law enforcement and security and the issue of transborder data flows, discussed in paragraphs 27-29 of the Consultation paper as the T-PD seeks to answer the question above, we ask that it consider the established and successful history of information sharing between European countries and the United States in the area of law enforcement and security without any history of abuse of personal data by law enforcement entities. In addition to the hundreds of bilateral information sharing agreements between the United States and the Council of Europe members, the United States has operational cooperative agreements with both Europol and Eurojust, European Union law enforcement bodies which cite Convention 108 as their authority for data protection.[309] The Council of Europe's 2002 *Report On The Third Evaluation Of Recommendation N° R (87) 15 Regulating The Use of Personal Data in the Police Sector*[310] states that fighting against serious crime constitutes a legitimate prevailing interest overriding the Convention's "adequacy" requirement for cross-border transfers, provided any agreement contains specific safeguards that protect data privacy in a manner consistent with the laws and policies of the concerned parties.

We respectfully request that any changes to the Convention continue to allow a degree of flexibility so that information sharing between the United States and European states and EU institutions can continue. Any revision of the Convention that is negotiated must include specific provisions that

[308] *Available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf.

[309] COUNCIL DECISION of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, Article 14 para. 2; and Council Decision of April 6 2009 regarding the European Police Office (Europol) Article 27.

[310] Report On The Third Evaluation Of Recommendation N° R (87) 15 Regulating The Use of Personal Data in the Police Sector done in 2002, paragraph 39.

authorize access to data and sharing of data between states for legitimate law enforcement and public security purposes. In addition, if these issues are to be discussed, delegations to the negotiations should include personnel who are experienced in how law enforcement and public security agencies use data on a daily basis to prevent, investigate and prosecute crime and terrorism.

VDZ (VERBANDS DEUTSCHER ZEITSCHRIFTENVERLEGER)

VDZ Verband Deutscher Zeitschriftenverleger

BDZV

Gemeinsame Stellungnahme
des Verbands Deutscher Zeitschriftenverleger
und des Bundesverbands Deutscher Zeitungsverleger
zur Konsultation des Europarates
zur Modernisierung der Konvention 108

Stand 10.03.2011

Der Verband Deutscher Zeitschriftenverleger (VDZ) ist der Dachverband der deutschen Zeitschriftenverlage. Die Mitgliedsverlage des VDZ geben insgesamt über 3000 Zeitschriftentitel sowie zugehörige Online-Angebote heraus und verkörpern damit rund 90 % des deutschen Zeitschriftenmarktes. Über 95 % der VDZ-Mitglieder sind kleine oder mittlere Unternehmen.

Der Bundesverband Deutscher Zeitungsverleger e.V. (BDZV) ist die Spitzenorganisation der Zeitungsverlage in Deutschland. Über seine elf Landesverbände sind dem BDZV mehr als 300 Tageszeitungen sowie 14 Wochenzeitungen einschließlich der zugehörigen Online-Angebote angeschlossen. Gemessen am Umsatz repräsentieren die BDZV-Mitgliedsverlage 85 % des deutschen Zeitungsmarktes.

Die deutschen Zeitschriften- und Zeitungsverleger nehmen gerne die Gelegenheit wahr, zu der Konsultation des Europarates zur Modernisierung der Konvention 108 (Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten) Stellung zu nehmen und werden sich dabei auf die Aspekte beschränken, die für Presseverleger von besonderer Relevanz sind.

1. Neue Herausforderungen für den Datenschutz und die Pressefreiheit

Datenschutz und Datensicherheit besitzen für Zeitschriften- und Zeitungsverlage einen hohen Stellenwert. Verbrauchervertrauen ist notwendige Voraussetzung für den Erfolg bestehender und neuer Geschäftsmodelle: Was im Zusammenhang mit den Printausgaben bereits seit Jahren selbstverständlich ist, gilt ebenso im Online-Bereich, in dem Nutzerreaktionen auf unseriöse Praktiken noch wesentlich schneller und unmittelbarer ausgedrückt und an einen großen Empfängerkreis weiter gegeben werden können.

Aus Sicht des VDZ und des BDZV ist bei der Auslegung, der Anwendung sowie etwaigen Überlegungen zur Weiterentwicklung des geltenden Rechtsrahmens jedoch auch sicherzustellen, dass die Pressefreiheit aus Gründen des Datenschutzes nicht weiter beeinträchtigt oder beschädigt wird.

Das Datenschutzrecht ist seit jeher für zwei wesentliche Bereiche der Pressetätigkeit relevant. Redaktionelle Pressefreiheit ist ohne Ausnahmen vom Datenschutzrecht nicht möglich. Und für den Erhalt der Leserschaft ist adressiertes Direktmarketing klassischer wie digitaler Presseabonnements unverzichtbar, das als Verarbeitung personenbezogener Daten dem Datenschutzrecht unterliegt.

Die Bedeutung der jeweils einschlägigen Datenschutz- und Datennutzungsregelungen für die Presse hat in den letzten Jahren zugenommen und wächst weiter. Hauptgrund dafür sind die mit der Digitalisierung verbundenen Umbrüche in der Mediennutzung, die die Verlage weiterhin vor bislang ungekannte Herausforderungen stellen. Insbesondere die allmähliche Verlagerung der Leserschaft

hin zu digitalen Endgeräten verlangt, dass die Presse ihre redaktionellen Inhalte auf allen relevanten Wegen verbreitet. Die deutschen Zeitschriften und Zeitungen, insgesamt mehrere tausend Publikationen, sind bereits heute fast ausnahmslos technologieneutral, d. h., sowohl im Einzelhandel und im Abonnement erhältlich als auch im Internet vertreten. Zusätzlich werden digitale Ausgaben über mobile Endgeräte wie Smartphones oder E-Reader angeboten. In publizistischer und funktionaler Hinsicht kann Presse nur noch in ihrer Mehrfachpräsenz auf Papier und digitalen Verbreitungswegen begriffen werden.

a) Robuste Bereichsausnahme für jede journalistische Datenverarbeitung erforderlich (Recherche, Archive, Herstellung und digitale Publikation)

Die Digitalisierung hat dazu geführt, dass eine robuste Bereichsausnahme vom Datenschutzrecht für jede journalistische Datenverarbeitung Minimum jeder Pressefreiheit ist.
Für die redaktionelle Pressefreiheit ist eine robuste Bereichsausnahme von den Datenschutzvorschriften unumgänglich. Diese muss technologieneutral alle Verbreitungswege und Medientypen und jede mit der Pressetätigkeit einhergehende Datenverarbeitung von der Beschaffung der Information und ihrer Archivierung im Redaktionsarchiv bis hin zur Verbreitung der fertigen Artikel und Publikationen – auch in digitaler Form – umfassen. Die Anwendung der Datenschutzvorschriften auf die journalistische Datenverarbeitung der Presse würde eine freie redaktionelle Berichterstattung in weiten Teilen unmöglich machen. Ein Großteil aller Informationen über Politik, Wirtschaft und sonstige Gesellschaft, die eine freie Presse frei sammeln, speichern und auswerten sowie veröffentlichen können muss, sind personenbezogen. Ein Großteil der Presseartikel, die den Kern der Aufgabe der Presse ausmachen und zum Wesen der Freiheit der Presse zählen, enthalten eine Vielzahl personenbezogener Daten.

So ist etwa die Information, dass Dr. Angela Merkel Bundeskanzlerin der Bundesrepublik Deutschland ist, ebenso ein personenbezogenes Datum wie der Umstand, dass sie im Bundeskanzleramt residiert. Die Tatsache, dass sie der Christlich Demokratischen Union angehört, wäre sogar als sensibles personenbezogenes Datum einzuordnen, da es Bezug zu ihrer politischen Überzeugung besitzt. Als sensibles Datum wäre beispielsweise auch die Information einzuordnen, dass jemand einer in bestimmter Weise politisch oder religiös motivierten Terrororganisation oder einer bestimmten religiösen oder politischen Sekte angehört, da diese Informationen die religiöse oder politische Überzeugung betreffen. Ebenso personenbezogen sind alle Informationen über Verfehlungen oder den Verdacht von Verfehlungen öffentlicher Personen, wie etwa Strafverfahren oder sonstige Anschuldigungen.

Die Zulässigkeit der Verarbeitung all dieser Daten zu journalistischen Zwecken muss nach wie vor und technologieneutral allein nach dem einschlägigen Äußerungs- und Medienrecht beurteilt werden, das ein angemessenes Instrumentarium enthält, Meinungsfreiheit und die jeweils einschlägigen Persönlichkeitsrechte abzuwägen. Das muss selbstverständlich auch für Zulässigkeit digitaler Verbreitungsvarianten der Presse gelten, sofern etwa die Verbreitung von Presseartikeln mit personenbezogenen redaktionellen Inhalten im Internet oder über mobile Endgeräte als Verarbeitung personenbezogener Daten verstanden wird. Bereits heute erreichen viele Zeitschriften und Zeitungen einen erheblichen Anteil ihrer Leserschaft auf digitalen Endgeräten, vielfach mit Artikeln, die identisch auch in der Papierausgabe erscheinen.

Eine Ausnahme für journalistische Datenverarbeitung muss sich ganz natürlich auf alle Einzelelemente der Konvention beziehen und insbesondere auch für zusätzliche Beschränkungen, die im Rahmen der Konsultation angedacht werden.

b) Angemessenes Datenschutzrecht für Pressevertrieb, Online-Werbung und sonstige unternehmerische Datenverarbeitung

Für die nicht-redaktionelle Verarbeitung personenbezogener Daten gilt selbstverständlich auch in Presseunternehmen das allgemeine Datenschutzrecht. Es hat allerdings ebenfalls im Zuge der Digitalisierung gerade für die Presse ganz erheblich an Bedeutung gewonnen, indem es über die Möglichkeiten des Pressevertriebs und bestimmter digitaler Anzeigen mitentscheidet, die ihrerseits in der strukturell schwierigen wirtschaftlichen Situation der freien Presse immer wichtiger werden. Auch dieser Sachverhalt soll kurz illustriert werden:

Der publizistische Erfolg der Presse ist ungebrochen. Zeitungen und Zeitschriften erreichen mit ihren Print- und Onlineausgaben sogar eher mehr Leser denn je. Der publizistischen Nachhaltigkeit steht jedoch bislang keine gesicherte Refinanzierung gegenüber. Werbeeinnahmen für die Onlineausgaben sind unverzichtbar, stellen aber lediglich Bruchteile der Einnahmen dar, die für Werbung in Printpublikationen erzielt werden. Vertriebserlöse der digitalen Presse sind ebenfalls dringend notwendig und werden wo immer möglich angestrebt und teilweise erzielt, bleiben aber für weite Bereiche der digitalen Presse jedenfalls derzeit kaum realisierbar. Da insgesamt die Online-Reichweite nur unzureichend zur Gesamtfinanzierung beiträgt, findet überwiegend eine Quersubventionierung statt, die mit der zunehmenden Verlagerung hin zu digitalen Ausgaben auf Dauer nicht funktionieren kann.

aa) In dieser Situation ist es umso wichtiger, dass Zeitschriften und Zeitungen unter angemessenen Bedingungen um neue Leser und Abonnenten werben können. Die Presse ist darauf angewiesen, je nach Titel eine natürliche Fluktuation von bis zu 30% der Abonnenten pro Jahr durch Direktmarketing über alle relevanten Kommunikationswege auszugleichen. Das Pressabonnement ist ein erklärungsbedürftiges Produkt ohne Ladenlokal, das die persönliche und also die adressierte Ansprache potenzieller Leser zwingend voraussetzt. Das Recht des Werbeadressaten, über die Nutzung seiner personenbezogenen Daten zu entscheiden, kann vielfach auch durch Information und Widerspruchsmöglichkeit in einen angemessenen Ausgleich mit berechtigten Interessen der Unternehmen gebracht werden. Um einen solchen Bereich handelt es sich etwa bei vielen Formen der Briefwerbung für Presseabonnements, von der bis zu 20% der Abonnementauflage von Titeln der Publikumspresse abhängen können.

bb) Werbeeinnahmen sind ein wesentliches Element der Finanzierung der freien und unabhängigen Presse. Werbeeinnahmen machen im Printbereich ca. 50 % der Einnahmen der Verlagshäuser aus, online sind es sogar bis zu 100 %. Vor dem Hintergrund der zunehmenden Verlagerung zur Online-Presse wird die Bedeutung der Werbung für die Finanzierung sogar noch zunehmen. Werbung muss daher auch weiterhin die zentrale Rolle einnehmen können, die sie für die Finanzierung der Presse innehat. Sichergestellt werden muss mithin, dass unter Verweis auf das Datenschutzrecht keine neuen Verpflichtungen eingeführt werden, die diese Möglichkeit ausschließen. Das gilt insbesondere auch für die Möglichkeiten interessenbasierter Online-Werbung.

2. Ausgewogener Ansatz für die Überarbeitung des Konvention 108 erforderlich

Insgesamt appellieren die deutschen Zeitungs- und Zeitschriftenverleger an den Europarat, bei der Überarbeitung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten einen ausgewogenen Ansatz zu wählen, der die bereits derzeit schon schwierigen Rahmenbedingungen für die Presse nicht noch weiter verschlechtert, sondern den Verlagen die Möglichkeit belässt, ihre bestehenden Angebote im Markt zu finanzieren und neue und nachhaltige Geschäftsmodelle zu entwickeln.

Datenverarbeitungsvorgänge sind mittlerweile zu einem wesentlichen Element unserer modernen, informationsbasierten Gesellschaft geworden. Datenverarbeitungssysteme tragen wesentlich zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels und zum Wohlergehen der Menschen bei. Für zahlreiche Wirtschaftsbereiche ist die Verarbeitung personenbezogener Daten Grundlage der täglichen Arbeit und für die konkurrenzfähige Bewältigung verschiedener Aufgaben unumgänglich.

Der Rechtsrahmen für das Grundrecht zum Schutz personenbezogener Daten muss auch diesen Erfordernissen Rechnung tragen. Die Anforderungen, die an Unternehmen gestellt werden, müssen nicht nur praktikabel sein, sondern dürfen die Unternehmen auch weder finanziell, noch personell oder technisch übermäßig und unangemessen belasten. Dies gilt insbesondere für kleine und mittlere Unternehmen, die bestimmte Anforderungen aufgrund des damit einhergehenden Aufwandes nicht bzw. nur schwerlich erfüllen können. Die Politik darf keine Vorgaben aufstellen, die letztendlich nur von wenigen international agierenden, nicht aber von der Mehrzahl der auf Datenverarbeitung angewiesenen Unternehmen erfüllt werden können.

ZENTRALVERBAND DER DEUTSCHEN WERBEWIRTSCHAFT ZAW E.V.

Der Zentralverband der deutschen Werbewirtschaft (ZAW) ist die Dachorganisation von 40 Verbänden der am Werbegeschäft beteiligten Kreise. Er vertritt die Interessen der werbenden Wirtschaft, des Handels, der Medien, der Werbeagenturen sowie der Werbeberufe und der Marktforschung. Er ist die gesamthafte Vertretung der Werbewirtschaft in Deutschland.

Der ZAW repräsentiert ca. 29 Milliarden Euro Investitionen in Medienwerbung und rund 550.000 Beschäftigte in den Arbeitsbereichen der Markt-Kommunikation. Zur Dachorganisation gehört auch der Deutsche Werberat, die zentrale Werbeselbstkontrolleinrichtung in Deutschland.

Dabei setzt sich der ZAW für die Freiheit der kommerziellen Kommunikation als einer unabdingbaren Voraussetzung für den im Interesse der Unternehmen und der Verbraucher liegenden unverfälschten und fairen Wettbewerb ein. Werbung und kommerzielle Kommunikation sind zugleich unverzichtbare Grundlage für die Finanzierung vielfältiger, unabhängiger Medien und somit ein wesentlicher Faktor für ein freiheitlich, demokratisches und nachhaltig verantwortungsbewusstes Gemeinwesen – in Deutschland wie auch in Europa. Mittels der Verantwortungsübernahme für die Werbeselbstkontrolle in Deutschland ermöglicht die im ZAW organisierte deutsche Werbewirtschaft zudem die Partizipation von Bürgern und gesellschaftlichen Gruppen am Prozess der Markt-Kommunikation und stellt zugleich ein effektives und effizientes Instrument des Konfliktmanagements zur Verfügung.

In seiner Stellungnahme beschränkt sich der ZAW nachfolgend auf die werbewirtschaftlich relevanten Aspekte.

I. Vorbemerkung

Der ZAW bedankt sich zunächst für die Gelegenheit, im Rahmen der Konsultation den aufgeworfenen Fragen einer Modernisierung der Konvention 108 des Europarats Stellung zu nehmen.

Einleitend möchten wir auch an dieser Stelle betonen, dass auf Basis der in der Konvention 108 enthaltenen Vorgaben nach Ansicht des ZAW bereits ein ausreichender Schutz der Betroffenen gewährleistet werden kann. Änderungen an der Konvention hält der ZAW daher nicht für erforderlich. Die Grundprinzipien des Übereinkommens haben sich bewährt. Wichtig ist, dass sie in der Praxis auch von allen Mitgliedern des Europarats umgesetzt werden.

Für die Werbewirtschaft ebenso wie für zahlreiche andere Wirtschaftsbereiche ist die Verarbeitung personenbezogener Daten unverzichtbare Grundlage der täglichen Arbeit. Hierbei sind die Normadressaten auf ein übersichtliches, verständliches und praktisch umsetzbares Datenschutzrecht angewiesen. Vor diesem Hintergrund betont der ZAW die Notwendigkeit, an der technologieneutralen Formulierung der Konvention 108 festzuhalten. Diese ist wesentlich, um auch künftig den sich aus der technologischen Entwicklung ergebenden Herausforderungen unmittelbar begegnen zu können.

Zu einigen der aufgeworfenen Fragestellungen nimmt der ZAW im Einzelnen wie folgt Stellung:

1. Angemessener Schutz des Einzelnen in allen Situationen

Ein angemessener Schutz personenbezogener Daten natürlicher Personen auch mit Blick auf die Entwicklung neuer Technologien ist bereits im Rahmen des geltenden Übereinkommens möglich. Eine Ausweitung des Anwendungsbereichs und damit die Einführung weiterer Vorgaben für Datenverarbeitungsprozesse sind – auch angesichts der zusätzlich bestehenden Regelungen zum Schutz der Betroffenen (z.B. EU-Datenschutzrichtlinie 95/46/EG) nicht erforderlich und würden zu einer unverhältnismäßigen Belastung von Unternehmen führen. Der ZAW spricht sich daher gegen jede Modifikation des Anwendungsbereichs aus, der zu einer weiteren Erschwerung von Datenverarbeitungsprozessen führen würde.

Im Übrigen erscheint es vor dem Hintergrund der fortschreitenden technischen Entwicklung zweifelhaft, ob statische (gesetzliche) Bestimmungen überhaupt das geeignete Regulierungsinstrument sind. Vorzugswürdig ist auch hier eine Stärkung der Selbstregulierung im Bereich des Datenschutzes, die in einem komplexen und dynamischen Wirtschaftsumfeld schnell, effektiv und flexibel auf aktuelle Entwicklungen reagieren kann. Jedenfalls sollten derartige, die Verarbeitung spezifischer Daten betreffende Bestimmungen keinesfalls in eine überarbeitete Konvention aufgenommen werden, da sonst die für den nachhaltigen Bestand des Rechtsrahmens erforderliche Technologieneutralität gefährdet wäre.

2. Mehr Transparenz für die von der Verarbeitung Betroffenen

Der gegenwärtige Rechtsrahmen sieht bereits ein hohes Maß an Information der Betroffenen und Transparenz über die Verarbeitung ihrer personenbezogenen Daten vor. Diese Bestimmungen wurden in Deutschland in nationales Recht umgesetzt und gewährleisten durch entsprechende Maßnahmen der Unternehmen in der Praxis bereits ein ausreichendes Maß an Transparenz bei der Datenerhebung.

Wir sehen auch die Gefahr, dass eine Ausweitung der schon bestehenden umfangreichen Informationspflichten der angestrebten Transparenz sogar abträglich sein und zur Verunsicherung und Verwirrung der Betroffenen beitragen kann. Ein Übermaß an Informationen, insbesondere auf einem komplexen Gebiet wie dem Datenschutz, kann bei dem Betroffenen leicht ein Gefühl der Überforderung, respektive Widerwillen hervorrufen mit der Folge, dass dieser die Informationen inhaltlich gar nicht mehr zur Kenntnis nimmt.

Insbesondere bei der Online-Kommunikation würden statische gesetzliche Pflichtvorgaben hinsichtlich der konkreten Modalitäten der bereitzustellenden Informationen nach Überzeugung des ZAW kontraproduktiv sein: Hier ist zu berücksichtigen, dass gesetzlich festgeschriebene Vorgaben den schnellen technischen Entwicklungen im Internet nicht Rechnung tragen können mit der Folge, dass diese gehemmt würden. Auch könnten starre Vorgaben der Informationsvermittlung den im Online-Bereich bereits vorhandenen sehr vielfältigen und zukünftig sich weiter ausdifferenzierenden Gestaltungsmöglichkeiten von Webangeboten nicht gerecht werden. Im Falle der Statuierung abstrakter Informationen im Rahmen von Datenschutzerklärungen an einem ebenfalls abstrakt für alle Onlineangebote bestimmten Ort auf einer Internetseite besteht wiederum die Gefahr, dass die Nutzer diese aufgrund ihrer Allgemeinheit und Komplexität letztlich gar nicht zur Kenntnis nehmen. Dies gilt auch und gerade für den in diesem Zusammenhang häufig beispielhaft angeführten Bereich der so genannten verhaltensorientierten Internetwerbung. Detaillierte – vom Europarat vorgegebene - Informationspflichten sind angesichts der technischen Komplexität und der Gestaltungsvielfalt dieser Onlineinhalte nicht geeignet, eine etwaige Verbesserung der Information der Betroffenen sicherzustellen.

Allenfalls erscheinen verstärkte Aufklärungsmaßnahmen der Betroffenen bezüglich eines verantwortungsvollen Umgangs mit ihren personenbezogenen Daten (Selbstdatenschutz) vorzugswürdig. Gegebenenfalls könnte auch durch Maßnahmen der Selbstregulierung der Datenschutz sowohl global als auch national effektiv und flexibel, z. B. durch die Vorsehung von kontext- und nutzerorientierten Informationen, gefördert werden.

3. Keine spezifischen Regelungen für Minderjährige erforderlich

Der ZAW ist ferner der Ansicht, dass spezifische gesetzliche Regelungen für den Schutz personenbezogener Daten Minderjähriger nicht erforderlich sind. Der bestehende Rechtsrahmen sieht bereits einen ausreichenden Schutz personenbezogener Daten vor. Zu Recht enthält die bisherige Fassung des Übereinkommens keine Altersgrenze. Fragestellungen beispielsweise im Zusammenhang mit dem Zustimmungserfordernis Minderjähriger können innerhalb des gegenwärtigen Rechtsrahmens auf europäischer und nationaler Ebene zufriedenstellend gelöst werden. Ob und inwieweit Daten aufgrund von Einwilligungen Minderjähriger erhoben, verarbeitet oder genutzt werden dürfen, ist vom Verwendungszusammenhang und von der üblicherweise von Kindern und Jugendlichen zu erwartenden Einsichtsfähigkeit abhängig zu machen. Ist eine minderjährige Person wegen ihrer körperlichen oder geistigen Fähigkeiten nicht in der Lage, Reichweite oder Folge der Zustimmung angemessen einzuschätzen, muss die Zustimmung bereits nach den geltenden Vorgaben durch entsprechend berechtigte Dritte – z.B. die Eltern – erteilt werden.

Schließlich erscheint insbesondere in Bezug auf Kinder die Förderung von Medienkompetenz durch entsprechende Aufklärungs- und Informationsmaßnahmen im Vergleich zur Statuierung weiterer gesetzlicher Informationspflichten vorzugswürdig. Diese Einschätzung entspricht aktuellen Erkenntnissen aus der Bildungsforschung. Anlässlich einer Anfang Dezember 2010 stattgefundenen Anhörung der Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestags haben Experten im Bereich der Medienpädagogik und

Bildungsforschung klargestellt, dass die Befähigung von Minderjährigen, mit den Herausforderungen neuer Medientechniken umzugehen, gegenüber stärkerer Regulierung und gesetzlichen Verboten klar den Vorzug verdiene[1]. Auf nationaler Ebene werden dieser Erkenntnis folgend bereits konkrete Maßnahmen zur Förderung der Medienkompetenz von Kindern und Jugendlichen umgesetzt: So wurde erst kürzlich ein Neustart der nationalen, von Bundesfamilien- und Bundesverbraucherministerium geförderten Online-Kampagne „watch your web" (http://www.watchyourweb.de/) durch die Bundesfamilien- und Bundesverbraucherministerin öffentlich bekanntgegeben[2]. Zusätzlich zu den bereits vorhandenen Maßnahmen sollten Aufklärungsinitiativen, insbesondere auf Selbstregulierungsebene anerkannt werden, die Minderjährige zu einem informierten und umsichtigen Umgang mit ihren Daten befähigen.

4. Bessere Kontrolle des Betroffenen über seine Daten

Nach deutschem Recht erstreckt sich seit der letzten Novelle des BDSG die Zielvorgabe des in § 3a BDSG geregelten Grundsatzes der Datenvermeidung und Datensparsamkeit über den Systemdatenschutz hinaus nunmehr generell auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Wenn die Möglichkeit zur Anonymisierung oder Pseudonymisierung besteht, so ist sie schon unter Erforderlichkeitsgesichtspunkten zu nutzen, solange deshalb kein unverhältnismäßiger Aufwand für die verantwortliche Stelle entsteht. Eine weitere Verschärfung dieser Prinzipien auf Ebene der Konvention 108 halten wir nicht für erforderlich.

5. Gewährleistung der Einwilligung ohne Zwang und in Kenntnis der Sachlage

Die gegenwärtige Anforderung einer „zweifelsfreien Einwilligung in Kenntnis der Sachlage" in der so genannten EU-Datenschutzrichtlinie stellt nach Ansicht des ZAW ein angemessenes Gleichgewicht zwischen dem in Artikel 8 der Charta der Grundrechte der Europäischen Union festgeschriebenen Recht auf Schutz personenbezogener Daten und dem in Artikel 16 der Grundrechtecharta verbrieften Recht auf unternehmerische Freiheit her. Eine solche Regelung hat sich auch weithin in der Praxis bewährt.

Überdies existiert hinsichtlich des Datenschutzes im elektronischen Bereich auf EU-Ebene bereits ein spezieller Rechtsrahmen in Form der E-Privacy-Richtlinie, deren Überarbeitung erst Ende 2009 abgeschlossen wurde und die nunmehr insoweit von den Mitgliedstaaten bis Mai 2011 in nationales Recht umzusetzen ist. Deren technologieneutrale Vorschriften gewährleisten einen umfassenden Schutz auch von personenbezogenen Daten im elektronischen Bereich und stellen auch im Übrigen die Vertraulichkeit der Kommunikation, unter anderem für die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits auf dem Endgerät eines Nutzers gespeichert sind, sicher. Es gilt nunmehr zunächst, diesen Regelungen auf nationaler Ebene in der Praxis zur Geltung zu verhelfen.

Um eine sachgerechte Balance zwischen der Möglichkeit der Nutzer, den Gebrauch ihrer Daten zu steuern, und den Kommunikationsnotwendigkeiten einer modernen Wirtschaft beizubehalten, muss hierbei stets berücksichtigt werden, dass die rechtskonforme Verarbeitung personenbezogener sowie anonymer Daten eine wichtige Rolle für verschiedene Online-Geschäftsmodelle spielt, mithin hierdurch attraktive und oftmals kostenlose Angebote im Internet erst ermöglicht werden. Dies gilt unter anderem auch für den von der Kommission beispielhaft angeführten Bereich der Online-Werbung. Fast sämtliche Medien (Werbeträger)

[1] http://www.heise.de/newsticker/meldung/Bildungsstunde-zu-Medienkompetenz-im-Bundestag-1152282.html
[2] http://www.bmelv.de/SharedDocs/Pressemitteilungen/2010/221-AI-Internet-Kampagne-watchyourweb-schillergymnasium.html

sind ebenso wie die werbewirtschaftlichen Dialogmarketingmaßnahmen heutzutage darauf angewiesen, auch online be- und vertrieben zu werden. Den dadurch enorm gestiegenen (Produktions- und Vertriebs-)Kosten stehen jedoch angesichts der vorherrschenden „Kostenlos-Mentalität" der Internetnutzer hinsichtlich einer Vielzahl von Online-Inhalten noch keine relevanten Vertriebserlöse in diesem Bereich gegenüber. Online-Werbung bildet daher ein unverzichtbares Element der Finanzierung freier und unabhängiger Medien auf deutscher und europäischer Ebene.

Eingedenk dieser Zusammenhänge kann unter anderem auch die Möglichkeit eines selbstregulativen Ansatzes der Internet- und Werbewirtschaft diskutiert werden, der durch die Festlegung differenzierter und praktikabler Maßnahmen hinsichtlich Transparenz und Wahlmöglichkeiten der Nutzer einen angemessenen Interessenausgleich zwischen allen Marktbeteiligten im Bereich der betroffenen Online-Werbegeschäftsmodelle herbeiführen kann. Diesem – in Übereinstimmung mit den spezifischen Vorgaben der E-Privacy-Richtlinie stehenden – Ansatz sollte im Falle einer etwaigen Überarbeitung der Konvention Rechnung getragen werden.

6. Schutz sensibler Daten

Eine Ausweitung des Katalogs sensibler Daten ist nicht erforderlich. In der Praxis bestehen vielmehr Probleme mit den geltenden Datenkategorien, weshalb auch nach Meinung des ZAW überlegt werden sollte, den Anwendungsbereich dieser Kategorien eindeutiger zu definieren. Bei einer solchen Präzisierung und Harmonisierung sollte jedoch nicht das Datum an sich die Schutzwürdigkeit vorgeben. Entscheidend für die Sensibilität der Daten ist – zumal aus der Sicht der Betroffenen – in der Regel der Kontext, in dem die Daten verarbeitet werden.

7. Grenzüberschreitender Datenverkehr

Untrennbar mit der Zielsetzung eines freien Verkehrs personenbezogener Daten verbunden ist die Tatsache, dass der Binnenmarkt den freien Wettbewerb zwischen Unternehmen sicherstellen will. Ohne Werbung aber ist freier Wettbewerb nicht möglich. Bei einer etwaigen Überarbeitung der Konvention muss deshalb aus Sicht des ZAW darauf geachtet werden, dass den Unternehmen ausreichend Möglichkeiten zum Direktmarketing bleiben, da andernfalls eine Stärkung des Binnenmarkts nicht möglich ist. Für die Werbewirtschaft ebenso wie für zahlreiche andere Wirtschaftsbereiche ist die Verarbeitung personenbezogener Daten dabei unverzichtbare Grundlage der täglichen Arbeit.

8. Die globale Dimension des Datenschutzes

Für international tätige Unternehmen ist es vor dem Hintergrund globaler Märkte von entscheidender Bedeutung, den internationalen Datentransfer zu erleichtern und zu vereinheitlichen. Es bedarf vor allem einfacher und verlässlicher Regelungen. International tätige Unternehmen benötigen ferner bestimmte Regelungen, die ihnen die interne Datenverarbeitung erleichtern. Der ZAW befürwortet daher die Aufnahme einer Konzernregelung in die Konvention 108.

Einzelstaatliche oder auch gemeinschaftliche Rechtsdurchsetzung endet an den Grenzen des Staates bzw. an denen der EU. Der Schutz des informationellen Selbstbestimmungsrechts liegt dagegen auch dann noch zuerst und weitgehend bei jedem Einzelnen. Der Ein-

zelne hat es weitgehend selbst in der Hand, wie viele und welche Daten über ihn z.B. im Internet verfügbar sind. Das beste und wirkungsvollste Mittel zum Schutz der Persönlichkeitsrechte bleibt deshalb der aufgeklärte (Internet-)Nutzer.