COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, le 2 avril 2012 T-PD-BUR(2012)03Mos

LE BUREAU DU COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL [STE n°108]

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

Modernisation de la convention 108 : compilation des commentaires reçus

Modernisation of Convention 108: compilation of comments received

DG I - Droits de l'Homme et Etat de Droit / Human Rights and Rule of Law

I – Membres du T-PD / T-PD Members

II- Observateurs

III- Autres réponses

MEMBRES DU T-PD / T-PD MEMBERS

AUTRICHE / AUSTRIA

1) General comments:

The Republic of Austria supports the modernisation of Convention 108 and wishes to underline that the European Union (EU) is currently modernising its legal framework on data protection as well. A close co-operation is therefore necessary and should be envisaged in order to avoid different approaches in this sensitive field of law between these two European organisations.

Convention 108 frequently refers to "domestic law". Given the fact that most Contracting Parties to Convention 108 are also members of the EU and that their law on data protection is primarily determined by Union law – currently in particular by Directive 95/46/EC and in the future perhaps by a directly applicable Regulation – the Republic of Austria invites the Bureau to reconsider references to "domestic law" in Convention 108 because there is very limited factual room of discretion for domestic law in this area for EU member states.

The following comments are made with reference to the proposals presented by the Bureau of the T-PD in document T-PD-BUR(2012)01Rev_en of 5 March 2012.

2) Comments on the Preamble and on Articles:

Preamble, Recital 4:
Having regard to the jurisprudence of the ECtHR on Art. 8 ECHR, the Republic of Austria is of the opinion that (the right to) data protection is also a human right and a fundamental freedom which exists alongside other rights guaranteed by the ECHR. Moreover, the right of data protection has recently acquired an autonomous meaning (see in this regard Art. 8 of the Charter of Fundamental Rights of the European Union and also Art. 16 para. 1 TFEU). Taking the jurisprudence of the ECtHR and the developments on the European level into account, Recital 4 should be rephrased, for example the following way:
"Recognising that it is necessary to reconcile the right to data protection and other human rights and fundamental freedoms…"

Article 2:
Generally, coherence and compatibility with the legal framework of the EU should be ensured, especially when dealing with definitions. Different approaches in this sector should be avoided and might have negative consequences. It is therefore proposed to harmonise – as far as possible – Art. 2 of Convention 108 and current Art. 4 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

Art. 2 (a): It should be mentioned in the Explanatory Report that an individual is not considered "*identifiable*" either, if identification can be carried out only with illegal means.

Art. 2 (c): It is proposed to insert the wording "*by automated means*" after "*…which is performed*" in order to make it clear that "*data processing*" refers only to "*automatic data processing*" and not to "*manual processing*".

The reference to a "*service provider*" on page 3 of the document should be eliminated because this term is not mentioned anywhere in the substantive part of the proposals.

Article 3:
The Republic of Austria strongly supports the provision of para. 1bis which is much better phrased that the comparable provision of Art. 2 para.2 (d) of the proposed General Data Protection Regulation but urges to sincerely reconsider the elimination of Art. 2 para. 2 (b) and (c) and paras. 3, 5 and 6.

For the sake of clarity and flexibility, states should have the option to extend the scope of data protection to persons or groups of persons other than human individuals (such as enterprises etc.). This should be stated directly in the Convention itself and not in the Explanatory Report.

Furthermore, if para. 2 (c) is eliminated, Convention 108 would fall behind the data protection standard of the EU (see currently: Art. 2 (b) of Directive 95/46/EC and also Art. 2 para. 1 and Art. 4 para. 3 of the proposed General Data Protection Regulation).

Article 5:
It should be considered to define "*consent*", either in Art. 2 or in the Explanatory Report. Examples for a definition can be found in Art. 4 para. 8 and Recital 25 of the proposed General Data Protection Regulation and Art. 2 (h) of Directive 95/46/EC.

The Explanatory Report should furthermore state that "*explicit consent*" can only be given for legitimate processing purposes. Processing for illegal purposes can never be covered by consent.

Article 6:
For the sake of legal certainty "*genetic data*" and "*biometric data*" should be defined in Art. 2 and not in the Explanatory Report (see also Art. 4 paras. 10 and 11 of the proposed General Data Protection Regulation). Furthermore, it could be envisaged to explain in the Explanatory Report that any data may become sensitive according to the purpose of the processing considered.

Article 8:
The Republic of Austria is of the opinion that Art. 8 (d) should be specified in a way to make it clear that a person cannot object to processing of personal data concerning him/her if there is a clear basis in law for data processing.

Article 8bis:
All measures mentioned in Art. 8bis concern controllers as well as processors. Therefore, processors should be mentioned in the text and in the title of Art. 8bis as well.

The italic text should read "*...could consist of the designation of 'data protection officers'…*" or "*…a 'data protection officer'…*" instead of "*…a 'data protection officers'…*".

Article 12:
The Republic of Austria supports the alternative proposal with the following amendments:

- The possibilities of para. 1 indents 1-3 are alternative, not cumulative; therefore, the word "*or*" should be inserted at the end of indents 1 and 2.

- Due to the wording of para. 4 ("*When the recipient is not subject to the jurisdiction of a Party…*") its relation to paras. 2 and 3 (the latter's beginning is likewise "*When the recipient is not subject to the jurisdiction of a Party…*") is not entirely clear. The Republic of Austria there proposes to have recourse to the wording of Art. 12 para. 4 on page 21 of the document which states "*Notwithstanding paragraphs 2 and 3…*".

Article 12bis:
Para. 3 should be amended in a way to make it clear that members and staff of supervisory authorities shall neither seek nor be subject to external instructions of anyone. Internal instructions are necessary for the internal administration of a supervisory authority (of course, internal instructions cannot be given to members when acting in their judicial capacity).

Para. 5 should be rephrased: Instead of "*effective remedies*" it would be better to refer to "*judicial review*" because otherwise Convention 108 might fall behind its current standard (see in this regard Art. 1 para. 4 of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows).

The wording "*explicitly agreed*" in para. 6 (a) should be replaced by "*given his/her consent*", because "*consent*" is a data protection term already used in the Convention.

The Republic of Austria would like to refer to Art. 51 and Recitals 97 and 98 of the proposed General Data Protection Regulation as one possible measure of cooperation between supervisory authorities within the meaning of para. 6 (b).

Furthermore, it should be mentioned in the Explanatory Report that supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 21:
The proposed new para. 7 of Article 21 introduces a new procedure for the entry into force of amendments, which is supposed to be an alternative procedure to that of para. 6. To make the relation of these two procedures more clear – either the one or the other procedure – we suggest to combine the two provisions in one paragraph.
Moreover, the word "*However*" at the beginnnig of para. 7 is not proper treaty language. It is suggested to replace it by the word "*Alternatively*".

Article 23:
This provision opens the possibility for International Organisations to accede to Convention 108. Para. 2 should therefore be properly amended and should speak of "*any acceding State or International Organisation*".

BULGARIE / BULGARIA

In connection with the sent request for review and comments on the newly proposed texts of Convention 108/81/CE for the protection of individuals with regard to automatic processing of personal data, the Commission for Personal Data Protection would like to make the following comments:

1. On Art. 5 "Legitimacy of data processing and quality of data", para.3 b)- we support the text but would like to be clarified that when data is processed for statistical, historical or scientific purpose is obligatory to be observed the requirement for the protection of the individual's privacy and other fundamental rights.

2. On Art. 6 "Processing of sensitive data"- to the sentence with which is set the exemption in the prohibition for sensitive data processing should be added as follows: "Such data may be nevertheless be processed where the domestic law provides appropriate safeguards and **where the processing is required by law.**" We are of opinion that the requirement for legitimacy and lawfulness of the processing of such data category is mandatory, because the national legislation may ensure the necessary measures for adequate personal data protection and despite that, in the particular case, their processing may not be lawful and necessary.

3. On Art. 7 "Data security", para.2- we support the inclusion of a text about the data subject notification obligation when serious risk occurs in the provision, not in the Explanatory Report.

4. On Art.7 bis "Transparency of processing", para.2 - to be clarified what is meant under "impossible" or "involves disproportionate efforts". We think that the individual's right of being notified about the personal data processing should not be limited unless the existence of serious ground and only in specific cases.

5. On Art. 9 "Exceptions and restrictions"- the wording of the text is not clear. At first glance it seems that the scope is too wide. We propose for more clarity, the explanations of the definitions to be included in the text of the provision and not in the Explanatory Report.
6. On Art. 9, para.2 and 3- to be included a text that the restriction in the freedom of expression and information (para.2) and the processing for statistical and scientific purposes

should be used only when the fundamental rights of the individual are guaranteed and especially the right of privacy.

7. On Art. 12 "Transborder data flows", para.4 c)- by the provision of data to third countries which do not have adequate protection level is foreseen a transfer when prevailing legitimate interests and especially important public interest exist. We are of opinion that in the provision should be well explained what is meant under "important public interest". In this regard the alternative version of the Art. 12 seem clearer but in it the above definition is also not clarified. This is important, because otherwise there is a treat of wide interpretation of the text and possibility to use it as ground for data transfer to countries which do not ensure adequate protection and also for misuse and unlawful processing.

8. On Art. 15 "Safeguards concerning assistance rendered by designated supervisory authority", para.3 - the reference to Art. 14 should be erased.

9.On Art. 16 "Refusal of requests for assistance"- the reference to Art. 14 should be erased.

As a conclusion, we would like to express our opinion that harmonization in the data protection provisions is needed in order to achieve effective application of the new European data protection legislation.

CHYPRE / CYPRUS

1. In preamble the term "privacy" is replaced by the term "dignity" we think that it would be preferable for both of the above terms to be included taking into consideration that a breach of privacy does not always lead to a breach of dignity.

2. As regards the term "jurisdiction" in article 1 which replaces the term "territory" provided for in the previous text we have forwarded a question to the Legal Service of Cyprus and we are expecting their reply so we retain our reservation. Special attention should be given with regard to the extra territorial jurisdiction.

3. As regards article 2 (c) "no automated processing" it should be rephrased as follows: "where no automated processing is carried out, data processing means the operations carried out within a structure set according to specific criteria which easily allows to search the data related to a specific subject". The specific criteria should be specified in the explanatory report.

4. With regard to article 5(3)(b) we consider that the word "specific" would be preferable instead of the word "specified" and before the word "processed" (second line) the word "further" should be inserted in order to give the correct meaning. In article 5(3)(e) is not clarified that data after the fulfillment of the purposes for which they have been processed are deleted afterwards.

5. With regard to article 7 bis "Transparency" it should be clarified in the explanatory report that transparency is one of the preconditions for fair processing but not the only one.

6. Referring to article 8 (c) which was not amended maybe a note on the right to be forgotten should be explained in the explanatory report.

7. With regard to article 8bis (first paragraph) it should be clarified who is responsible for taking all appropriate measures the controller or the processor in the case the processing is delegated to a processor and by what means? What is exactly meant by the phrase "observe the domestic legal provisions"?

8. Article 9(3) refers to restrictions on the exercise of the rights included in articles (6, 7bis and 8). However article 6 does not provide or refer to any rights instead article 6 refers to the processing of sensitive data. The other 2 articles 7bis and 8 provide for data subjects' rights so the phrase "on the exercise of the rights specified" should be deleted in order to provide the correct meaning. In addition the phrase "where there is obviously no risk" should be rephrased as follows: "when there are no obvious risks".

9. There should be an amendment in article 10 in order to provide for the right of the data subjects to appeal to the competent courts.

10. Article 12 (3)(b) in order to achieve a uniform application and avoid private assessments of adequacy on a case by case basis the provision of standardized or ad hoc legal measures should be developed by the Council of Europe (T-PD) and should have the legal form of standard contractual clauses approved by the European Commission or at least a similar measure. Respective amendments should be carried out in article 19 regarding the functions of the committee. As for article 12(4) (a) before the word "consent" the word "explicit" should be added in order to exclude the

possibility of implied consent being allowed and in 6th line of the present paragraph the words “data subjects” should be replaced by the words “personal data” since speaking about adequate level of protection we mean adequate level of protection of personal data and not data subjects. A general reservation regarding article 12(3) procedure is that the supervisory Authority should have a more active role specifically prior to the transfer of data. Comparing the provisions of article 12(2) to those of 12(3) it seems that the transfer of data to a party to the Convention that has not implemented all or some of the rights and obligations enshrined therein is more restrictive than the transfer of data to a recipient who is not subject to a jurisdiction of a party to the Convention.

11. Alternative proposal does not meet the necessary requirements for the transfer so it is not supported.

12. We strongly support the provisions with regard to the Supervisory Authority independence added in article 12bis (3) and (4).

13. In Article 19 (h) the word “may” should be deleted and be replaced by the word “shall” according to our comments in paragraph 10 above.

FRANCE

L'approche qui consiste à maintenir le caractère général et technologiquement neutre du texte tout en veillant à son application effective est indispensable nous semble t-il pour permettre la pérennité du texte et sa large application au niveau international. A cet égard il paraît important de veiller à ne pas introduire de dispositifs contraignants qui serait un frein à son application internationale ou qui pourraient limiter les ratifications.

La cohérence à l'égard de l'évolution des autres textes européens est à privilégier sans perdre de vue toutefois la nécessité de conserver ses caractères propres à la Convention 108. De ce fait le rapport explicatif devra permettre d'apporter tous les éléments de précision nécessaires afin de conserver au texte de la Convention son niveau général. Notamment il devra expliquer pourquoi on ne trouve pas explicitement le droit à l'oubli mais comment on a privilégié l'existence de moyens qui permettent l'effectivité de ce droit tout en veillant à ne pas porter atteinte au droit d'information et d'expression.

Il conviendrait aussi que le rapport explicatif précise que le but poursuivi est de faire en sorte que la protection des données s'applique à toutes les étapes de la chaîne des traitements des données et aux intervenants principaux dans cette chaîne.

Il devra expliquer le basculement opéré par rapport à la situation actuelle où la personne a désormais un droit de contrôler ses propres données ce qui est un signe important pour l'interprétation de la Convention par la Cour européenne des droits de l'Homme.

Enfin, il devra reprendre les tendances qui ressortaient des réponses à la consultation publique. Les intervenants ayant exprimé leur attachement à ce texte.

Préambule:

2° paragraphe : le rapport explicatif devra veiller à expliciter ce que l'on entend par "droit de contrôler ses propres données" : portabilité des données et contrôle de l'utilisation qui est faite des données.

6° paragraphe : Ce paragraphe ne trouverait-il pas plutôt sa place dans le rapport explicatif en raison des différences nationales actuellement sur ce sujet et de la situation de ratification de la Convention sur l'accès aux documents publics. Par ailleurs, en énonçant ce principe se trouve posée la question de savoir s'il n'y a pas d'autres principes qui devraient être pris en compte.

Pour le rapport explicatif il est prévu de faire référence à la Résolution de Madrid. De manière générale ou à certains points de la Résolution ?

Article 2 : Pas d'observation particulière. La définition large de la notion de données à caractère personnel de la Convention a résisté au temps et trouve encore à s'appliquer dans la mesure où elle englobe à la fois la notion de personne concernée et de donnée. La

précision sur le fait de pouvoir individualiser une personne paraît importante dans le rapport explicatif pour compléter la notion d'identifiable.

Art 2c : une proposition rédactionnelle en français pour la deuxième partie ."Lorsque aucun procédé automatisé n'est utilisé le traitement de données s'entend des opérations effectuées sur des données à caractère personnel organisées de manière structurée selon des critères déterminés"

Art.2 f. : Sauf erreur de ma part, on ne trouve de conséquence de cette définition du sous traitant que dans les articles 7 et 8. L'objectif poursuivi est-il de lui appliquer toutes les obligations qui reposent sur le responsable de traitement.? Si c'est bien le cas, on devrait le retrouver partout ailleurs dans le texte quand on parle du responsable de traitement, sinon on laisse croire que les obligations ne s'appliquent pas à lui. Le rapport explicatif ne pourrait-il pas indiquer que la notion de responsable de traitement englobe le sous traitant? Ce peut être une position de prudence par rapport aux évolutions technologiques qui feront que d'autres acteurs pourront être impliqués dans le processus de traitement des données. L'impact de la Convention est en effet d'offrir les définitions les plus larges de manière à éviter d'être dépassée par la technologie.

Art 5 2 b). Les deux cas visés par ce b) sont très différents. Je proposerai de scinder cet alinéa en deux .

Dans le rapport explicatif il est prévu de traiter du caractère rétractable du consentement. Il pourrait être utile que sous le a) le rapport précise tout particulièrement que le responsable de traitement a la charge de la preuve du consentement et qu'il doit fournir une information spécifique sur les conditions et les modalités de retrait du consentement.

Enfin, dans cet article on parle de consentement "spécifique, libre et éclairé" et dans le 3 b) on parle du consentement "explicite"

Sur la notion de "finalités compatibles" qui doivent être précisée dans le rapport explicatif, il ne s'agit pas que de finalités statistiques, scientifiques etc... Cette finalité peut aussi couvrir le cas d'une finalité seconde déterminée par le responsable de traitement et qui est compatible avec la finalité première sans être pour autant nécessairement exprimée.

Art .7 2 : Il faudrait que la proposition faite de notifier a tout le moins aux autorités de contrôle soit en conformité avec les textes européens. La Convention 108 peut prévoir le principe de notification mais sans entrer dans le détail de la procédure afin d'éviter tout conflit avec d'autres textes.

Par ailleurs on parle de "violations de sécurité". Veut-on parler de violations de failles de sécurité ou, comme le projet de Règlement de violation de données à caractère personnel ? L'adverbe "gravement" peut soulever des interrogations. Il faudrait l'expliciter dans le rapport explicatif

Je propose pour la fin de cet article de dire "susceptibles de porter atteinte (gravement) aux droits et libertés fondamentaux" par cohérence avec le Préambule.

Art.7 bis 1 : Parmi les informations fournies par le responsable de traitement se trouve "le principal établissement". Eu égard aux difficultés rencontrées dans la projet de règlement sur cette notion, il conviendrait de trouver une autre expression d'autant que dans le cas de la Convention 108 , cette notion n'a pas de conséquence directe en termes d'accès pour les personnes ou de rôle des autorités de protection

Je propose de compléter cet alinéa par l'indication que le responsable de traitement fournit l'information "au moment de la collecte des données ou à tout moment à la demande de la personne". Cette idée est exprimée dans le 8a). Il serait peut-être plus lisible de la remonter ici d'autant que l'information n'est pas stricto sensu un droit de la personne mais une obligation du responsable de traitement

Art 7 bis 2 proposition de rédaction "le responsable de traitement n'est néanmoins pas tenu de fournir ces informations lorsque cela implique des efforts disproportionnés". L'expression "lorsque cela lui est impossible" entraîne une interprétation très subjective sur l'impossibilité de faire. Je propose donc de supprimer cette expression.

Art.8 : Proposition rédactionnelle en français : "obtenir à intervalle raisonnable et sans délai ou frais excessifs la confirmation ou non de l'existence d'un traitement la concernant, la communication sous une forme intelligible des données collectées et traitées, ainsi que les informations disponibles sur l'origine des données".

Dans cet article, je proposerais d'intervertir les alinéas de la façon suivante : mettre le e) en a) car il s'agit d'un principe général de base, et le d) en b).

Comment l'alinéa actuel d) sur l'opposition "a tout moment" s'articule-t-il avec le consentement explicite préalable et rétractable ?

Art.8 Bis : Proposition de modifications de l'intitulé de l'article "Obligations du responsable de traitement" par exemple. Par ailleurs, les obligations citées dans cet article ne vise pas uniquement le responsable de traitement mais aussi le sous traitant . Il ya un problème de cohérence qui rejoint la question posée sous l'article 2f.

Pourquoi le 3è paragraphe de cet article ne vise pas aussi le sous- traitant ?

Concernant les flux transfrontières de données, les propositions reflètent la volonté de veiller à la libre circulation des informations tout en assurant l'application de la Convention. Elles doivent rester technologiquement neutres, à l'instar du reste de la Convention pour pouvoir aussi s'appliquer notamment au Cloud computing sans en restreindre la mise en œuvre.

Article 18 Comité Consultatif. Je propose de placer le i)en b) pour distinguerr clairement ce que le comité fait de son propre chef de ce qu'il fait à la demande de tiers.

art 18 h) Quel est le sens de cet alinéa.?

LITUANIE / LITHUANIA

1. Change term “General orientations” into “General remarks”.

2. Supplement paragraph on main objectives:
“…to deal with challenges for privacy **and personal data protection** resulting from the use of new ICTs;…”

3. Supplement part of the “Supervisory authorities” introducing and defining detailed criteria on independence of the Supervisory authorities, especially having in mind that those criteria are introduced in the proposed new EU Regulation on data protection. The same applicable to the Paragraph 4 of Article 12bis.

4. Consider whether in text of the Convention in Preamble provided guarantee “as well as everyone’s dignity” shall be left, or whether it would be more convenient to supplement data subject rights or even introduce new article on Evaluation of Personal Aspects by Automatic Means.

5. In Article 6 “Processing of sensitive data” consider whether all biometric data shall be prohibited of processing, except if domestic law provides appropriate safeguards, as such regulation can be burdensome for example to the photographers and photo salons.

6. Revise Paragraph 2 of Article 12, because part where is provided cases when presumption of adequacy shall not operate can be confusing and not always properly executed.

7. In Paragraph 4 c) of Article 12 delete words “in particular public interests” because such term as a public interest is not introduced and it would be difficult to estimate whether public interest prevails.

8. Supplement Paragraph 5 of Article 12bis: “…effective remedies **and may be appealed against trough the courts**.”

9. In Paragraph 6 a) delete “or that the data subject has previously explicitly agreed to” because if exchange of the personal data is not essential for cooperation such data shall not be exchanged at all.

10. Consider whether Paragraph 6 b) shall be introduced as a duty and not as a right of the supervisory authority.

MONACO

S’agissant de la citation du principe du droit d’accès aux documents publics dans le préambule, j'attire votre attention sur le fait que la convention sur l’accès aux documents publics n’a eu à ce jour que peu de ratifications et que l’adhésion à la convention 108 modifiée ne saurait indirectement faire reconnaître un tel principe. Monaco dispose d'un régime juridique complet sur l'accès aux documents administratifs mais n'a pas adhéré à la convention sur l'accès aux documents publics. Aussi, afin d'éviter le télescopage entre les champs d'application des deux conventions, il m’apparaît préférable de biffer cette disposition ou de la compléter par les dispositions suivantes : « Considérant que la présente Convention permet aux Parties qui l’ont adopté de prendre en compte, dans la mise en œuvre des règles qu’elle pose, le principe du droit d’accès aux documents publics. »

Dans l’introduction, la référence à une définition du prestataire devrait être supprimée, car celle ci ne figure pas dans le corps du texte et aucune obligation spécifique ne semble plus leur être attribuée.

S'agissant de soumettre les responsables de traitement à une obligation d'analyse de risque avant de procéder à un traitement pouvant présenter un risque particulier pour les personnes concernées, je m'interroge sur les difficultés de mise en oeuvre que cela entraînerait non seulement pour les petites et moyennes entreprises, mais aussi pour les petits Etats qui ne disposent pas des structures et moyens nécessaires pour procéder, dans tous les cas, à une analyse d'impact.

Au b de l'article 12 bis, la suppression des termes "à caractère personnel" dans le périmètre de saisine des autorités de contrôle par une personne d'une demande relative à la protection de ses droits apparaît contradictoire avec le champ d'application de la Convention et son titre lesquels visent expressément "les traitements de données à caractère personnel"

La Principauté ne serait pas opposée aux propositions de modernisation en faveur d’une plus grande harmonisation des critères de légitimité et de qualité des données, de transparence, sécurité des données et droits des personnes concernées. Elle n’a pas d’objection au renforcement des pouvoirs du Comité Consultatif.

Elle est attentive à l’objectif poursuivi par la Convention de recherche de cohérence et de compatibilité de la Convention avec le cadre juridique de l’Union européenne, afin de favoriser les flux transfrontières.

NORVEGE / NORWAY

The Norwegian delegation has a question relating to article 5 of the latest modernization proposals for Convention 108, with reference to the general objective to ensure for coherence and compatibility with the legal framework of the European Union which is listed in the introduction to the modernization proposals. It is unclear to us whether article 5 number 2 of the proposal, is meant to limit the possible grounds for lawful processing of personal data, compared to directive 95/46/EC and the General Data Protection Regulation proposed by the Commission (COM (2012) 11 final). It is also unclear to us whether the scope of article 5 number 3 b is narrower than the scope of article 6 number 4 of the proposed General Data Protection Regulation.

We are also wondering if the compatibility with the General Data Protection Regulation has been examined with regards to the proposed article 8 b (on obtaining knowledge of the logic involved in the data processing in the case of an automated decision) and article 8 e (on the right not to be subject to a decision based solely on the grounds of an automated processing of data).

We hope that the Bureau can take these questions into consideration when finalizing the proposals, and to address these issues at the next plenary meeting of the T-PD.

PORTUGAL

Article 9 – Exceptions et restrictions

Une nouvelle exception est proposée pour le traitement des données à caractère personnel aux seules fins de communication au public d'informations, d'idées ou d'opinions d'intérêt général, ou à des fins d'expression artistique ou littéraire. Les exemptions des exigences de certaines dispositions sont nécessaires pour concilier le droit à la protection des données avec la liberté d'expression. (et autres droits ?)

- développer ses activités normatives en agissant comme un forum international pour discuter de questions émergentes et s'entendre sur des approches communes face aux nouveaux défis pour la vie privée, en particulier résultant du développement des TICs, développant des lignes directrices et des recommandations applicables à des secteurs spécifiques tels la biométrie, les assurances, les données médicales ou la police (entre autres);
-

Article 2 – Définitions	**Article 2 – Définitions**
Aux fins de la présente Convention:	inchangé
a «données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»);	Inchangé *Compléter le rapport explicatif, notamment pour préciser qu'une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais ou des activités déraisonnables pour une personne qui en prendrait connaissance* *Préciser également que par « identifiable » on n'entend pas seulement référer aux éléments de l'identité civile d'un individu mais aussi et plutôt à ce qui permet d'individualiser une personne parmi d'autres. (NON. C'est précisément de l'identification civile qu'il s'agit.)*

(Article 3 – Champ d'application)

1 Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé.	1 Chaque Partie s'engage à appliquer la présente Convention aux traitements de données effectués par tout responsable du traitement relevant de sa juridiction. 1 bis La présente Convention ne s'applique pas aux traitements de données effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques, à moins que les données ne soient rendues accessibles à des personnes ne relevant pas de la sphère personnelle ou domestique. *Dans le rapport explicatif, préciser ce que l'on entend par exercice d'activités exclusivement personnelles ou domestiques et accessibles à des personnes ne relevant pas de la sphère personnelle ou domestique.* *Préciser que le traitement concerne des*

	données à caractère personnel mais que les parties ont (selont sont Droit interne) ~~néanmoins~~ la possibilité d'étendre la protection aux personnes morales.

(Article 5 – Légitimité des traitements de données et qualité des données)

b enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;	b **collectées** pour des finalités explicites, déterminées et légitimes et ne pas être **traitées** de manière incompatible avec ces finalités **à moins d'avoir obtenu le consentement explicite de la personne concernée ou que cela soit prévu par le droit interne;** *Dans le rapport explicatif, donner des exemples de finalités compatibles (la finalité statistique, historique ou de recherche scientifique est a priori compatible pour autant que d'autres garanties légales soient prévues et que le traitement ne serve pas à prendre une décision à l'égard d'un individu)Une certaine recherche scientifique visant combattre une certaine maladie qui à pris, au delà des donnés rendus anonymes, ceux d'un certain malade identifié qui a accepté de collaborer consciemment finira par le bénéficier.*

Article 9 – Exceptions et restrictions	**Article 9 – Exceptions et restrictions**
1 Aucune exception aux dispositions des articles 5, 6 et 8 de la présente Convention n'est admise, sauf dans les limites définies au présent article.	1 Aucune exception aux dispositions de la présente Convention n'est admise, sauf aux articles 5.3, 6, 7.2, 7bis, et 8 et à condition qu'une telle dérogation soit prévue par la loi et constitue une mesure nécessaire dans une société démocratique : *Rapport explicatif : une mesure sera considérée comme « nécessaire dans une société démocratique » pour atteindre un but légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants ». NON. Qui va juger, face à un pays souverain si un but est légitime où non ? et selon quel critère sera déterminée là légitimité ?quelle est le critère pour déterminer la pertinence et la suffisance ?* *Il y a seul un critère possible, le respect pour les droits de l'homme interprétés à là lumière de la Convention Européenne des Droits de l'Homme, des Statuts du Tribunal Pénal Internationale, la jurisprudence de la Cour Européenne des Droits de l'Homme, où celle de la Cour Pénale Internationale.*

(Proposition alternative)

	4. Lorsque le destinataire ne relève pas de la juridiction d'une Partie à la Convention, la communication ou mise à disposition des données peut se faire lorsqu'une des dérogations suivantes s'applique : a) la personne concernée a donné son consentement, après avoir été informée des risques dus à l'absence de garanties appropriées ; ou b) des intérêts spécifiques de la personne concernée le nécessitent ; ou c) des intérêts légitimes protégés par la loi, en particulier des intérêts publics importants, prévalent. Mettre en ligne avec le projet de Règlement de l'Union Européenne.

RÉPUBLIQUE DE MOLDOVA / REPUBLIC OF MOLDOVA

On behalf of the National Center for Personal Data Protection of the Republic of Moldova I would like to inform about the sustaining of the proposals on modernisation of Convention 108. Also we think that the alternative proposal on wording of the art. 12 is more acceptable.

RÉPUBLIQUE TCHÈQUE / CZECH REPUBLIC

Article 2 … **Definitions**

c …data processing… means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data;

Be careful with the listening of operations – use similar wording with the new EC Directive; it will be helpful for implementation of documents.

Article 6 … **Processing of sensitive data**

Stress more than a list of sensitive data importace of the context in which data are used - important for the sensitivity of data

Article 9 … **Exceptions and restrictions**

1
a protect State security, public **security**, the **economic and financial** interests of the State

Possibility of excessive use – rights of citizens can be under unaproppriate pressure.

Supprimé : or¶
the **prevention** and suppression of criminal¶ offences;

Article 25 … **Reservations**

Make admissible upon Vienna Convention on the Law of Treaties (Art. 19 -_23)

ROYAUME-UNI / UNITED KINGDOM

Art 6 – sensitive data
The wording in this article leaves no room for a risk and context-based approach. We suggest adding wording to this kind of provision to say that it does not apply where the processing has no significant or adverse effect on the individual. Also, biometric data is not always sensitive data and can in fact be used to provide a more privacy friendly approach. The recent Article 29 opinion makes some valid points about the definition of biometrics and it is worth bearing this in mind for the definition in C108.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf (page 10) (apologies, I am unable to copy and paste the text)

Article 7 – data security
The word 'accidental' has been crossed out and it is not clear why you wouldn't want organisations to put in place security measures to prevent against accidental loss of data. This seems to be a step backwards from current law and practice. With regards to data breach notification, CoE should bear in mind the work being done elsewhere on this topic to make sure that the Convention is in line with other practice, to avoid confusion and conflicting requirements.

Article 9 – derogations from the principles, sensitive data, transparency to individuals, and access rights
We have some concern about being able to derogate entirely from all the principles and other aspects above. Current law encourages derogations from these aspects 'to the extent that it would prejudice…' which avoids a blanket approach being taken that may deny individuals legitimate rights and access to their data.

Article 12 – transfers and national supervisory authorities
We are concerned by the development in article 12(3) that sets out that supervisory authorities shall be informed of measures taken in relation to transfers. This should only be where national law provides that this should happen. Arrangements for ensuring adequate levels of protection for transfers are the responsibility of the organisation transferring the data. If the arrangements are sent to the supervisory authority, there is an expectation that the authority will do something with them, be that proactive approval or silence indicating approval. We do not feel this is an appropriate role for the supervisory authority. We would prefer the wording of the alternative proposal (starting on page 21).

12 bis (7) – authorities forming a conference
We would hope that the explanatory memorandum makes clear that regard should be had to existing opportunities for authorities to meet and discuss relevant matters. The privacy and data protection calendar is already full and we would be wary of encouraging another separate event.

Article 19(d) – consultative committee
The revised wording generally as well as in this article has given the consultative committee more presence and power, which is not necessarily negative. However, if they are to start giving opinions on the interpretation of the Convention, as well as its application, then it might be worth having wording (perhaps in the explanatory memorandum) that they should ensure consistency with interpretations on the same or similar subjects given by other bodies

or committees. Otherwise you might find they have a different view on a key aspect to the Art 29 WP, the Commission, Court decisions and so on, which will cause confusion.

SLOVÉNIE / SLOVENIA

With regard to the text of the proposed changes for the modernisation of the Convention 108 as contained in the document T-PD-BUR (2012)01Rev of 5 March 2012, the following comments and changes are proposed.

PREAMBLE

In the fourth recital the following changes are proposed:

"Recognising that it is necessary to balance data protection and human rights and fundamental freedoms, notably the right of access to official documents and freedom of expression which includes the freedom to receive and impart information, regardless of frontiers;"

Supprimé : reconcile

Explanation
We find the expression »balance« more convenient to »reconcile« since the latter seems rather vigorous in this context. In addition to the »freedom of expression«, we propose also stressing the right of access to official documents being singled out as a special modern right by the Council of Europe Convention on Access to Official Documents.

Ad Article 6

After the proposed two paragraphs we propose an additional (third) paragraph reading:

»In the event that sensitive personal data cannot be separated from other categories of personal data, these data may exceptionally be processed in accordance with appropriate safeguards under domestic law, but prohibited criteria from the first paragraph shall not be the primary purpose for their processing.«

Explanation
It is sometimes impossible to separate sensitive from the non-sensitive personal data - like when a data subject is paying with a credit card, issued by a trade union savings bank ("other beliefs"), or maybe when a colour photo of person`s face is processed, which shows a colour of the skin.

Alternatively, we agree with the explanation of this kind of cases in the explanatory report, like it has been already proposed to illustrate the functional aspect of data becoming sensitive according to the purpose of the processing considered.

SUISSE / SWITZERLAND

Remarques générales

Nous saluons le travail de modernisation de la Convention et de son protocole additionnel et nous soutenons l'approche suivi tendant à maintenir la nature générale et technologiquement neutre des dispositions de la Convention tout en assurant la cohérence et la compatibilité avec le cadre juridique de l'Union européenne. La suite de la procédure d'élaboration et de l'adoption du texte doit se faire de manière à garantir cette indispensable cohérence. Compte tenu du fait que la Convention doit pouvoir offrir un standard international minimum et uniforme garantissant un niveau élevé de protection des données et susceptible de rallier le plus grand nombre d'Etats, la ligne actuelle suivie doit être maintenue. Le bureau est néanmoins invité à considérer, autant que possible et en tenant d'autres intérêts spécifiques, tels que la poursuite pénale et de la coopération judiciaire, la possibilité de rendre certaines dispositions de la convention d'application directe. Nous pensons en particulier aux dispositions relatives aux principes de base de la protection des données, aux droits des personnes concernées et aux obligations de transparence. En outre sans nécessairement réintroduire la possibilité de déclarations excluant certains types de traitement du champ d'application de la convention, il conviendrait de s'assurer que le projet tienne suffisamment compte des besoins spécifiques de la poursuite pénale et de la coopération policière et judiciaire, notamment en développant autant que nécessaire l'exposé des motifs au titre de l'article 9. Il devrait également examiner l'opportunité d'introduire une disposition sur le droit applicable.

Remarques spécifiques

Le titre de la Convention doit correspondre au nouveau champ d'application :

Convention pour la protection des personnes à l'égard du traitement ~~automatisé~~ des données à caractère personnel

Préambule
Au considérant 2, nous proposons la rédaction suivante :

Considérant qu'il est nécessaire, eu égard à **la diversification et** l'intensification des traitements **ainsi que** des échanges de données à caractère personnel, de garantir la protection des droits et des libertés fondamentales, ainsi que de la dignité de chacun, notamment au moyen du droit de contrôler ses propres données **et les usages qui en sont faits.**

Dans le rapport explicatif, la référence aux décisions automatisées doit être un exemple de traitements qui sont de nature à porter atteinte à la dignité des personnes.

Article 2, lettre c

Dans l'exposé des motifs, il faudra expliciter l'expression « l'application d'opération logiques et / ou arithmétiques aux données » en tant que phase du traitement de données.

Dans l'exposé des motifs, il conviendra également de préciser que l'expression « dont la structure permet de rechercher les données par personne concernée » concerne non seulement le cas où nous avons affaire à un classement par personne concernée, mais également d'autre types de classement qui permettent de rechercher les personnes ayant la même caractéristique (classement par localisation, profession, âge, etc.).

Article 3

Dans l'exposé des motifs, il conviendra d'expliquer pourquoi nous proposons d'abandonner le régime des déclarations au sens de l'art 3, al. 2, let. a. En particulier, il convient de rappeler que dans le texte

actuel, une Partie a la possibilité de déclarer qu'il n'appliquera pas la convention à certaines catégories de fichiers automatisés de données à caractère personnel, dans la mesure où ces fichiers ne sont pas assujettis. Cette disposition n'est pas conçue pour exclure de manière permanente des fichiers ou des traitements, sauf à introduire des réserves, ce que les auteurs de la convention ont exclus : des dérogations n'étant possible qu'en vertu de l'article 9. Il conviendra ainsi de prêter une attention particulière à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Art. 3, al. 1bis

Pour l'EM, préciser que les produits et services offerts aux fins de la mise en œuvre de tels traitements sont soumis aux principes de la convention.

Article 4

Nous proposons d'ajouter à l'article 4, al. 1, le chapitre IIIbis. En effet l'exigence d'une autorité de contrôle indépendante fait partie du « noyau dur » de la protection des données.

Nous proposons de modifier l'article 4, al. 2 comme suit : « Ces mesures doivent être prises avant l'adhésion ou la ratification » En effet, si on veut permettre au T-PD d'émettre un avis préalable à une adhésion, il est nécessaire que les mesures nécessaires à donner effet aux principes de base pour la protection des données soient déjà adoptées.

Article 5

A l'instar de l'article 5, alinéa 3, lettre b, nous proposons d'ajouter à l'alinéa 1 « légitime » après « finalité ».

Concernant le consentement prévu à l'article 5, alinéa 2, nous proposons de préciser dans l'exposé des motifs qu'il doit être explicite s'il s'agit de données sensibles au sens de l'article 6.

Article 6

Nous proposons de modifier la fin de la deuxième phrase de l'article 6 comme suit :

« ainsi que les données à caractère personnel reconnues par une Partie comme présentant un risque grave pour les **intérêts, les droits et les libertés fondamentales** de la personne concernée, … » La notion de risque grave est vague. Dans l'exposé des motifs, il faudra préciser dès lors ce que l'on entend par risque grave et donner des exemples afin d'éviter une interprétation trop divergente entre les Parties.

Concernant la définition des données biométriques, nous proposons de reprendre, dans l'exposé des motifs, la définition du projet de règlement européen (« toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telle que les images faciales ou des données dactyloscopiques. »

Article 7

Nous proposons la formulation suivante pour l'article 7, alinéa 1 :

« Chaque Partie prévoit que … prennent des mesures de sécurité appropriées **contre la modification ou la destruction accidentelles ou non autorisées des données à caractère personnel, ainsi que contre la perte et l'accès ou la diffusion non autorisés de telles données**. »

Dans l'exposé des motifs, il convient de préciser que les mesures doivent être adaptées à la nature des données traitées et aux risques d'atteintes aux droits et libertés fondamentales. Il faudra en particulier tenir compte dans l'évaluation du risque du fait que les donnés relèvent ou non d'un secret protégé par la loi.

A l'article 7, alinéa 2, nous proposons la rédaction suivante :

« Chaque Partie prévoit que le responsable du traitement … les violations de sécurité des données **de nature à** porter [gravement] atteinte **aux intérêts ou aux droits et libertés des personnes concernées**. »

Dans l'exposé des motifs, il faudra donner quelques exemples d'atteinte grave. En outre si dans le texte de l'article 7, alinéa 2, nous maintenons l'expression « gravement », il faut adapter l'exposé des motifs qui prévoit l'information des personnes concernées en cas de risque grave ou alors prévoir dans la disposition, comme dans le projet de règlement européen et le projet de directive obligatoirement l'information des personnes concernées, ce qui à notre avis va trop loin et peut-être problématique.

Article 7bis

A l'article 7bis, alinéa 1, nous proposons de rajouter l'information sur les « données traitées »

Concernant l'exposé des motifs en relation avec l'alinéa 2, nous proposons de préciser non seulement le moment de l'information (en règle générale lors de la collecte), mais également le comment : en particulier l'information faite en ligne doit être évidente et non pas par des renvois à des liens que personne ne va lire. Concernant les informations sur les transferts éventuels à l'étranger, elles devraient inclure les mesures prises pour garantir le respect des droits des personnes concernées.

Il convient d'examiner, en particulier lors de collecte de données auprès de tiers, une exception au devoir d'information lorsque que la collecte est prévu par la loi et que celle-ci contient les éléments essentiels de l'information.

Article 8

Dans l'exposé des motifs relatif à l'article 8, lettre a, nous proposons de préciser que « la forme intelligible » s'entend tant au regard du contenu de l'information que de la forme de la communication « sous format informatique standardisé » en fonction du contexte et pour assurer le caractère loyal de l'exercice du droit d'accès.

Nous proposons de modifier l'article 8, lettre b comme suit :

« obtenir connaissance de la logique qui sous-tend le traitement de données **dont les résultats lui sont opposés** » [variante : « obtenir connaissance du raisonnement utilisé dans le traitement dont les résultats lui sont opposés. »]

Dans l'exposé des motifs, nous pouvons préciser que ce droit peut être limité, lorsque cela est nécessaire dans une société démocratique pour préserver des secrets protégés par la loi, au lieu de dire que cela ne doit pas se faire au détriment de ces secrets.

Concernant l'article 8, lettre g, il conviendrait de préciser dans l'exposé des motifs que ce droit d'assistance peut être limité au titre de l'article 9, ou aménagé de manière à préserver les intérêts d'une procédure judiciaire pendante. Quant au contenu de la demande, nous proposons d'ajouter

dans l'exposé des motifs également les éléments en possession du requérant qui permettent de caractériser le ou les traitements de données auxquels sa demande se réfère.

Article 8bis

Nous proposons de numéroter les alinéas.

A l'alinéa 1, nous proposons de remplacer « observer » par « mise en œuvre ».

Dans l'exposé des motifs au titre de l'alinéa 4, préciser que le chargé à la protection des données doit exercer sa mission de manière indépendante.

Nous nous demandons dans quelle mesure il n'y aurait pas lieu de compléter l'article 8bis par une disposition spécifique concernant les producteurs et les fournisseurs de services qui reflète les exigences du « privacy by design or privacy by default » et qui pourrait avoir la teneur suivante :

« Chaque Partie prévoit que les produits et les services destinés au traitement de données à caractère personnel et diffusés sur ou à partir de leur juridiction, doivent comporter des fonctionnalités simples d'usage et permettant d'assurer la conformité des traitements de données au regard du droit applicable sur leur juridiction. »

Article 9

Concernant l'exposé des motifs au titre de l'alinéa 1, nous proposons d'ajouter après « besoin social impérieux » qui ne peut être atteint par des moyens moins intrusifs ».

Il faudra prêter un soin particulier dans l'exposé des motifs relatif à l'alinéa 2 pour bien expliciter la portée des dérogations au titre de l'article 9. En particulier concernant les procédures judiciaires en matière pénale, et/ou la coopération policière et judiciaire, il conviendrait de reprendre les motifs de restriction énoncés dans l'article 11, chiffre 4 et 13 chiffre 1 du projet de directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données du 25 janvier 2012. En outre, il faut s'interroger sur la nécessité de prévoir dans l'article 9 ou dans l'article 12bis, une possibilité d'exclure du champ de compétence des autorités de contrôle les traitements effectués par les juridictions dans l'exercice de leurs fonctions juridictionnelles (du moins tant que le traitement se réfère à une procédure pendante) (voir art. 44, chiffre 2 du projet de directive européenne susmentionnée).

Article 12

Nous trouvons la version principale plus claire. Elle a dès lors notre préférence.

A l'article 12 alinéa 2 (version française), remplacer « données personnelles » par « données à caractère personnel ».

A l'article 12, alinéa 4, ajouter « données à caractère personnel » après « la mise à disposition ». En outre, nous proposons de restreindre le transfert de données au cas particulier. Il ne devrait en effet pas permettre des échanges de données de manière régulière, répétitive et massive. En outre dans l'exposé des motifs, il faudra préciser ce que nous entendons par intérêts légitimes protégés par la loi en reprenant et complétant l'exposé des motifs du protocole additionnel. En particulier, il peut s'agir des motifs de l'article 9, lettre a et notamment de transferts nécessaires à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites pénales ou d'exécution de sanctions pénales. Il devrait également couvrir le transfert nécessaire à la constatation, à l'exercice ou à la

défense d'un droit en justice en rapport avec la prévention et la détection des infractions pénales, des enquêtes et des poursuites pénales ou de l'exécution de sanctions pénales.

Article 12bis

Nous proposons de compléter l'article 12bis, alinéa 1 en introduisant un devoir de sensibilisation et d'information des personnes concernées et des responsables de traitement. Nous proposons également d'examiner la possibilité pour les autorités de contrôle de prononcer des sanctions.

Nous proposons de modifier l'alinéa 4 comme suit :

« Chaque Partie s'assure que les autorités de contrôle disposent de ressources humaines, techniques et financières adéquates et des infrastructures nécessaires **pour exercer leurs missions et leurs pouvoirs de manière autonome et effective**. »

A l'alinéa 7, nous proposons de biffer « peuvent » : « …se constituent en conférence. » En effet, la formulation actuelle risque de rester lettre morte. Or si on estime que la coopération entre autorités est indispensable pour assurer au niveau international l'effectivité de la protection des données, il faut prévoir cette structure de coopération.

Comme indiqué sous article 9, il faut s'interroger sur la nécessité de prévoir dans l'article 9 ou dans l'article 12bis, une possibilité d'exclure du champ de compétence des autorités de contrôle les traitements effectués par les juridictions dans l'exercice de leurs fonctions juridictionnelles (du moins tant que le traitement se réfère à une procédure pendante) (voir art. 44, chiffre 2 du projet de directive européenne susmentionnée).

Article 18

Dans l'exposé des motifs au titre de l'alinéa 2, nous proposons de préciser que les représentants au comité devraient avoir une expérience ou des connaissances dans le domaine de la protection des données.

A l'alinéa 3, nous sommes d'avis que la majorité absolue des représentants habilités à voter serait suffisante. Une majorité des 2/3 nous parait trop élevée et difficile à atteindre. En outre dans l'exposé des motifs, il convient de préciser qui peut avoir le rang d'observateur.

Article 19

Nous saluons la mise à jour et le renforcement des compétences du comité pour lui permettre de jouer un rôle plus marqué dans la mise en œuvre de la convention. Dans l'exposé des motifs, nous proposons de préciser que le comité consultatif a également pour rôle de suivre les évolutions technologiques, sociales et économiques et juridiques en relation avec la mise en œuvre de la convention et qu'à ce titre, il peut être amené à adopter des recommandations.

Concernant l'article 19, lettres e et f, il convient de préciser dans l'exposé des motifs que l'avis devra être élaboré selon une procédure transparente et loyale vis-à-vis de l'Etat ou de l'organisation concernée et sur la base de critères objectifs.

Article 20

Nous proposons d'adapter l'alinéa 1 à la pratique actuelle : « … Il se réunit par la suite au moins une fois par année et … »

OBSERVATEURS / OBSERVERS

International Chamber of Commerce *(Christopher Kuner)*

1. With regard to the so-called "right to be forgotten" or "right to oblivion", I propose that the following text from page 5 of the Introduction (slightly modified) be incorporated into the explanatory memorandum:

> "The Convention does not provide for an explicit inclusion of a 'right to be forgotten' or 'right to oblivion'. It was felt that the existing safeguards (notably article 5.e concerning the length of time of data storage, and article 8.c concerning right of rectification or erasure of data) coupled with an effective right of opposition would offer adequate protection."

I have already heard people in the data protection community ask whether the CoE would incorporate the right to be forgotten into Convention 108, and for the historical record I think it is important to make it clear that this possibility was considered but ultimately not adopted.

2. In the Preamble, I suggest adding a paragraph stating that data protection must be balanced with other fundamental rights in light of the principle of proportionality, here is a suggested text:

> "Recognising that, like any fundamental right, the right to the protection of personal data must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality,"

The above language is taken from Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke* [2010] ECR I-0000, paras. 48, 50, and 86.

3. With regard to Article 3.1bis concerning the scope of the Convention and the exemption for data processing carried out in the exercise of purely personal or household activities, I think that in the explanatory memorandum it should be specified that whether data are made accessible to an indefinite number of persons is a relevant factor to be taken into consideration when determining whether the exemption applies. This is in accordance with ECJ cases C-73/07 *Satakunnan, Markkinapörssi and Satamedia,* [2008] ECR I-09831, and C-101/01 *Bodil Lindqvist,* [2003] ECR I-12971.

4. I like both of the two proposals for Article 12, though I prefer the alternative proposal. Here are some specific points:

--Article 12.2., second paragraph: the second sentence refers to the "Party invoking this clause", but it isn't clear if this means a Party being accused of not adequately implementing the Convention, or one making such an accusation against another Party. In addition, shouldn't there be some mention of how such a lack of implementation can be raised? Finally, it is not clear what "paragraph 3b" refers to, is this Article 12.3.b below?
--Article 13.3.b: I would be in favor of keeping the language in square brackets, but modifying it to read "or if this is not the case that the recipient implements all relevant legal measures that are feasible and likely to contribute to protection of the data subjects".

AUTRES REPONSES / OTHER ANSWERS

ARD / ZDF

März 2012

Stellungnahme der Arbeitsgemeinschaft der öffentlich-rechtlichen Landesrundfunkanstalten der Bundesrepublik Deutschland (ARD) und des Zweiten Deutschen Fernsehens (ZDF)

Modernisierung der Konvention 108 (T-PD-BUR(2012)01Rev_en)

Executive summary

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 German public service broadcasters our main concerns with regard to the draft document of the Convention (T-PD-BUR (2012) 01Rev_en) are the following *(we also would like to refer to our position paper of March 2011 on the previous consultation of the Council of Europe):*

Respect the important role public service broadcasting play for democracy by ensuring universal access to impartial news and a diverse range of high-quality content. In order to fulfil this important role, effective independence from governments must be ensured, including full independence with respect to data protection.

Creation of a fair balance between the fundamental right of privacy (Art. 8 ECHR) and the right of freedom of expression and the proper working of the media (Art. 10 ECHR).

Maintaining broadcasting specific data protection supervision which is provided by their proper independent control bodies, rather than by State authorities. This is owed to the requirement of independence of the media laid down in Art. 10 ECHR and ensures highly effective control.

In order to take account of these concerns and equally in order to guarantee consistency and compatibility with EU legal framework and especially the current EC draft regulation, ARD and ZDF suggest amending Article 9 (1b) (see proposal in the Annexe).

ARD und ZDF begrüßen die Initiative des Europarates, die geltende Datenschutzkonvention (Konvention 108) zu modernisieren. ARD und ZDF begleiten und beobachten intensiv den Diskussionsprozess zum Datenschutz sowohl auf Ebene des Europarates als auch in der Europäischen Union.

Zunächst ist es von Bedeutung, noch einmal auf die besondere Rolle des öffentlich-rechtlichen Rundfunks für die **Medienfreiheit** und dessen Faktor für die **Demokratie** hinzuweisen. Diese besondere Rolle und die Notwendigkeit einer auch organisatorischen und strukturellen Unabhängigkeit öffentlich-rechtlicher Medien von staatlichen und sonst fremden Einflüssen wurden zuletzt noch einmal in der Europaratsdeklaration vom 15. Februar 2012 hervorgehoben. Darin heißt es unter anderem:

"In a democratic society, people should be able to understand, contribute to and participate in the decision-making processes which concern them. Public service media play a fundamental part in sustaining this right through their mandate to ensure, via the relevant modes of delivery, universal access to impartial news and a diverse range of high-quality content which meets the needs of the wide variety of audiences."[1] und weiter:

"As an important public source of unbiased information and diverse political opinions, public service media must remain independent from political or economic interference."

Zu der Freiheit der Medien und der besonderen Rolle des öffentlich-rechtlichen Rundfunks zählt es auch, 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.

Deswegen halten es ARD und ZDF für nötig und unterstützen es, wenn in dem vorgelegten Konventionsentwurf eine Balance zwischen dem Grundrecht auf Privatheit (Artikel 8 EMRK) und dem Grundrecht auf Informations- und Meinungsfreiheit (Artikel 10 EMRK) geschaffen wird.

Die Verwirklichung der Meinungsfreiheit spiegelt sich in Deutschland auch darin wider, dass die Datenschutzaufsicht bei ARD und ZDF durch rundfunkeigene, völlig unabhängige Kontrollstellen wahrgenommen wird. 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**.

[1] Declaration of the Committee of Ministers on Public Service Media Governance, adopted by the Committee of Ministers on 15. February 2012 at the 1134th meeting of the Ministers' Deputies.

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 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.

Insbesondere im Hinblick auf eine erforderliche parallele Entwicklung des Rechts des Europarates und der Europäischen Gemeinschaft (Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr KOM(2012) 11 endgültig) sowie der notwendigen Rechtssicherheit erscheint eine Ergänzung der Europaratskonvention in Bezug auf die Möglichkeit der spezifischen nationalen Ausgestaltungen der Datenschutzbehördengeboten.

Annex - Änderungsvorschlag

Article 9 (1b) Exceptions and restrictions

T-PD-BUR(2012)01Rev_en	ARD/ZDF proposal
Article 9 b protect the data subject or the rights and freedoms of others, notably freedom of expression and information.	b protect the data subject or the rights and freedoms of others, notably freedom of expression and information *as well as the functioning of the media.* *In this respect exceptions to Article 5.2. and Article 12bis should be provided in order to ensure the freedom of the media and a highly effective control.*

Australian Privacy Foundation's International Committee *(Graham Greenleaf)*

Introduction

We support the objectives of the review, and particularly the objective to 'reaffirm the Convention's potential as a universal standard and its open character.'
The advantages of the 'globalisation' of Convention 108 (developing it into a global data privacy agreement, open to all contries providing an appropriate level of data protection) to countries outside Europe are significant, but only if an appropriately high level of privacy protection is required for non-European accessions. This perspective is argued in detail in Greenleaf (2012), and this submission adopts the views taken in that article as background.
This Submission endorses the proposals set out in 'Modernisation of Convention 108 – New Proposals' (T-PD, March 2012) except insofar as they are discussed and criticised in the following submissions. We have also given specific endorsement below to proposed positive changes that are of particular importance. The submission follows the order of the Convention text.

Article 1 – Object and purpose

Whether focus is placed on 'territory' or 'jurisdiction' there will be complex issues of delineation. The term 'jurisdiction' is, however, preferable in light of the nature of modern communication technologies, and we support its use.

Article 2 – Definitions - "Personal data"

The proposed Explanatory Report note should be amended by the addition of words such as "Reasonableness of time and effort required for identification must be considered relative to the privacy interests which may be adversely affected if in fact identification does take place, and to the commercial or other factors which may encourage attempts at identification."

Article 3 – Scope

The proposed change "to fully apply the Convention whenever personal data is accessible to persons outside the personal or domestic sphere" is supported strongly.
The deletion of rights of derogation is also supported strongly.

Article 4 – Duties of the Parties

(1) The words "on the basis that the State has taken the necessary measures in its domestic law to give effect to the basic principles for data protection" are the key to whole Convention, at least insofar as accession by non-European States is concerned. It is essential that the Explanatory Statement should clarify that the 'necessary measure' taken do in fact (in practice) 'give effect' to the basic principles, and not merely as a matter of passage of legislation. In the context of EU 'adequacy' determinations, terminology such as 'a good level of compliance', 'provision of appropriate redress' and 'provision of support and help' are used to indicate the substantive effect that is required.

(2) The comment by the Consultative Committee that "Whether all …necessary measures… have been taken will be scrutinised a priori by the Consultative Committee, in order to ensure that the conditions for the free flow of data are met" needs to be incorprorated into, and elaborated on, in the Explanatory Report to the revised Convention, to ensure that all parties acceding to the Convention (particularly non-European parties) are aware that accession is not merely a matter of formal legislative enactment.

Article 5 – Legitimacy of data processing and quality of data

We support strongly the requirement of proportionality in processing in propsoed Article 5(1). We support strongly the wording used to describe the consent requirement in 2(a) ('the data subject has freely given his/her specific and informed consent').

Article 10 – Sanctions and remedies

Why is no change proposed here? The requirement of the 2001 Additional Protocol (ETS 181) that individuals have a right of appeal to the Courts is not being incorporated into the revised Convention. This is a backward step. The words "(include a right of appeal to a Court)" should be inserted after "domestic law".

Article 12 – Transborder data flows

The proposed Article is supported, and the 'Alternative proposal' is very strongly opposed. In our view, adoption of the 'Alternative proposal' creates the possibility that Civil Society organisations will oppose the Convention becoming a global data privacy Convention, instead of supporting this. Comments on both versions follow.

(1) The proposed revision (supported, subject to necessary clarifications): The proviso to 3(b) is not sufficiently clear. Strong support is given to the condition of prior disclosure of 'accountability' measures to the competent supervisory authority, so that it can test (and accept or reject) them. This is essential to stopping 'adequacy' becoming the private assessment of the party with something to gain from making it. In 4(c), 'consent' should be replaced with 'explicit consent' so as to exclude the possibility of implied consent being allowed. Preferably, the same wording should be used as in proposed Article 5 2(a) ('the data subject has freely given his/her specific and informed consent'), or a general definition of 'consent' in these terms should be included in the Convention.

(2) The alternative proposal (opposed, irrespective of modifications): The proviso to 2 is inadequate because it does not require that protections be implemented by law, leaving 'adequacy' to be some vague notion of being observed in practice. 'Rights and obligations' are created by law, not practice, and it is doublespeak to pretend otherwise. Sub-clause 3 is fraudulent, because it is based on a (hypothetical) request from a supervisory authority that has no means of knowing that the transfer has ever happened, and therefore no reason to ever request a demonstration of 'accountability'. This is the bogus version of accountability at its most blatant. Here, the transferor has only 'adduced adequate safeguards' to its own satisfaction (and its own benefit), safe in the knowledge that its judgement will never be likely to be put to the test (or in the unlikely worst case, only after the damage is done). This alternative should be rejected completely.

The application of Article 12 also would benefit from further clarification of the meaning of the phrase 'a recipient who is not subject to its jurisdiction'. The data protection schemes of several countries cater for extraterritorial application (see e.g. the recent EU proposal, the Australian legislation, and the recent proposal for a privacy regulation in Singapore). In other words, such regulatory schemes claim jurisdiction over foreign organisations in certain circumstances. There may then be a risk that it could be argued that the communication, or making accessible, of data to such organisations does not fall within the regulation of Article 12 as the recipient accessing the data is in fact subject to the jurisdiction of the country from which the data is accessed. This would be undesirable, because the effective reach of extra-territorial laws may fall short of the effectiveness of its territorial application.

Article 18 – Composition of the committee

This change is supported strongly. It is important that Civil Society and Business observers be able to be invited. The change should say "voting", not "entitled to vote", given the difficulty that the Consultative Committee seems to have in getting responses from members, if the Uruguay accession is any indication. To do otherwise would be a *de facto* veto of non-State observers.

Article 19 – Functions of the committee

(1) In proposed item (d) the deletion of "at the request of a party" is supported strongly. The Committee should be able to issue opinions of its own motion.

(2) Proposed item (e) is supported strongly, and (as already stated in relation to Article 4), the basis on which the Committee draws up such opinions needs to be clarified in Article 4 and in the Explanatory Statement. It should state that any such opinion shall be made public.

(3) Item (f) should state that (i) such evaluation is for the purposes of Article 12, and (ii) any such evaluation shall be made public.

(4) Item (g) needs clarification: How can the Committee assess whether the standards set out in Article 12 offer sufficient guarantees, when they are deemed to do so? Presumably what is meant here is the preparation of a report (pursuant to Article 12(2)) on whether a particular country's standards offer such guarantees, whether the report is requested by the country concerned, or by another country.

Article 23 – Accession by non-member States or international organisations

(1) Following the words "accede to this Convention", the words "on the basis that the State has taken the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this Convention" should be inserted. If such words are not inserted, then (in theory) the Committee of Ministers could invite any State, no matter what its level of data protection, to accede. Furthermore, without such a clear statement of the basis of accession, there is no clear standard against which the Consultative Committee must prepare its report, and the criteria for accession by non-member States could be weaker than for member States..

(2) The Explanatory Statement should set out in detail what factors the Consultative Committee is likely to take into account in preparing its opinion, and in particular that that it is an opinion not only on formal legal measures but also includes an assessment of the extent to which data protection is delivered in practice in order to 'give effect' to the 'basic principles'.

(3) In particular, it should be made clear that an opinion of the Consultative Committee is not made on the same basis as the EU's WP29 opinions on 'adequacy'. The basis of an Article 23 opinion must be the provision of data protection to the citizens of the acceding country, not the adequacy of protection to European citizens.

Canadian Internet Policy & public Interest Clinic *(Tamir Israel – Staff lawyer)*

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
University of Ottawa – Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa|ON|K1N 6N5
cippic@uottawa.ca
www.cippic.ca

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. Pursuit of its public interest mandate includes expert testimony before parliamentary committees, interventions in Canada's judicial system, appearances and submissions to various tribunals such as the Office of the Privacy Commissioner of Canada, and participation in international Internet governance bodies. In addition, CIPPIC advises clients (organizational and otherwise) on matters with a public interest dimension and provides public education resources on various legal issues.

Privacy and data protection have been central to CIPPIC's mandate since its inception. CIPPIC's organizational experience includes active participation in the development and ongoing modification of Canada's federal data protection statute, the Personal Information Protection and Electronic Documents Act (PIPEDA). 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 Internet Service Provider customer's data for the purpose of traffic management using Deep Packet Inspection network equipment, the implications 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.

While Canada is not a member of the Council of Europe, nor is it a signatory of Convention 108, the Canadian government participates in CoE activities by virtue of its status as an Observer State. More importantly, as in most areas of Internet governance, we cannot live in splendid isolation and the policies of one governance body will often impact on others with like-minded ideas and values. With this in mind, CIPPIC offers the following comments based on its domestic experience with Canada's data protection regime as well as on relevant experiences in international policy-making venues.

Generally, CIPPIC commends the Council of Europe on adopting a balanced set of proposals for the modernization of its privacy protective framework. Our selective comments here supplement our initial comments of March 10, 2011,[1] and are restricted to those areas where our institutional experience is deemed to be of greatest potential benefits. Lack of comment on a specific provision should not be taken as endorsement thereof. It is our hope that our comments below are helpful.

Article 2 – Definitions

The document intends to narrow the definition of 'personal information' in order to provide guidance on the limits of data protection principles in an age where de-anonymization is almost always a real and tangible risk. This should only be done with great caution, as too great a limitation may well exclude many privacy harms that should rightfully remain subject to data protection principles.

The proposal intends to clarify, in the explanatory report, that 'personal information' excludes anonymized data that cannot be linked to an individual without 'unreasonable time or effort'. This raises

[1] CIPPIC, "Comments on the Modernization of Convention 108", Submission to Consultation on the Council of Europe's Discussion Paper, March 10, 2011, <http://www.cippic.ca/sites/default/files/20110310-CIPPIC-Comments-Conv108.pdf>.

concerns, as it may not provide adequate protection for personal information. For example, it may fail to account for scenarios where specific interest in a specific individual might justify an 'unreasonable' amount of time and effort, such as in the case of a nosy neighbour attack, or if there is organizational interest in identifying a specific sub-category of individuals. As 'personal information' is the gatekeeper of data protection regimes, it is important to adopt a broad and expansive definition so as not to exclude categories of information best left within the scope of the statutes.

The express inclusion of data capable of facilitating 'individualisation' is a welcome clarification, and adequately addresses online scenarios where tracking is largely traceable back to an anonymous identifier. However, the inclusion of this qualifier does not in and of itself alleviate all concerns raised by the 'unreasonable time or effort' standard.

Consideration should be given to adopting a higher standard. Canadian jurisprudence, for example, has converged on a definition of personal information that applies wherever "there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information."[2]

Article 3 - Scope

The document proposes to exempt private conduct from the Convention's scope. Specifically, 'purely personal or household activities' are to be exempted unless the data is "made accessible to persons outside the personal or household sphere."

CIPPIC agrees that limiting the scope of data protection regimes to exclude purely private activities may be justified. While the capacity of individuals to injure each other's privacy has grown significantly in a web 2.0 environment, data protection regimes are far better designed and suited to ensuring accountability in organizations than in inter-personal interactions. PIPEDA, Canada's data protection regime, is limited in application to an transaction or course of conduct that is of a commercial character.[3] With respect to the particular line drawn in proposed changes to Article 3, including information 'made accessible to persons outside the personal or household sphere' appears intended to ensure that while private user interactions (social network interactions) are excluded, commercial activities of those entities that facilitate these interactions (the social network itself) remain subject to the regime.

This should remain the guiding principle for any demarcation aimed at excluding private conduct. Proposed Article 3 suggests the possibility that this 'private conduct' exception be extended to all 'legal persons'. This appears to imply the inclusion of corporations which, if it is the case appears at first glance to have great potential for undermining the careful demarcation indicated in proposed 1bis of Article 3.

Article 5 – Legitimacy of data processing

The document envisions the adoption of a consent regime. This should be undertaken with great caution. The proposal does well to limit data processing to scenarios that are proportionate and

---

[2] Office of the Privacy Commissioner of Canada, "Interpretations: Personal Information", Last updated October 2011, <http://www.priv.gc.ca/leg_c/interpretations_02_e.cfm >.

[3] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, paragraph 4(1)(a).

necessary to legitimate objectives. It should be made clear, at the outset, that consent does not override a data controller's obligation to ensure data processing is proportionate and necessary to achieve a legitimate objective.

The definition of consent could benefit from added clarification on what constitutes 'freely given, specific and informed'. It should be manifestly clear that 'informed' consent entails more than mere 'notice' and does not import concepts developed in the context of contract law. Consideration should be given to 'meaningful consent' as a better defined standard. Further, 'time' of consent is important in this context and merits specification in either the Article or its accompanying explanatory note. Consent should be premised on information provided prior to the initiation of any data processing (or as soon as is practically possible thereafter).[4]

Further, in an online environment, the viscosity or 'effort' associated with achieving a privacy-friendly service configuration is critical.[5] In this context, subtle changes in privacy settings or in the mechanisms by which consent is sought can have dramatic impact on citizens' privacy choices.[6] It leads to privacy practices conducted under the superficial appearance of 'consent' but which depart dramatically from user expectations of how their data is actually being processed.[7] It then becomes critical to ensure that 'quality of consent' obligations recognize impact. Recognizing the principle of 'privacy by default' will help achieve this objective.[8] Privacy by default is a concept that obligates data controllers to assume

---

[4] For examples of 'time of consent' provisions, see the *Personal Information Protection and Electronic Documents Act*, , S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, Schedule 1, Principle 4.2.3: *"The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes."*

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Council Recommendation, September 23, 1980, <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>, Part Two, paragrpah 9: *"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."*

[5] See Office of the Privacy Commissioner of Canada, "Report on Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing", May 2011, <http://www.priv.gc.ca/resource/consultations/report_201105_e.pdf>.

[6] See R.H. Thaler & C.R. Sunstein, "Nudge: Improving Decisions About Health, Wealth, and Happiness" (Michigan: Caravan Books, 2008), for a description of the impact of 'effort' on economic efficiency and customer choice, generally. See L. Church & A. Whitten, "Generative Usability: Security and User Centered Design beyond the Appliance", *NSPW 2009*, <http://www.nspw.org/papers/2009/nspw2009-church.pdf> for a description of the impact of interface design and viscosity on user choices (albeit in the context of security, not privacy. For more privacy-specific examples see I. Kerr, J. Barrigar, J. Burkell, & K. Black, "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent", in I. Kerr, V. Steeves, & C. Lucock, *Eds., Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford: 2009, Oxford University Press), <http://idtrail.org/content/view/799> and A. Acquisti & J. Grossklags, "Privacy and Rationality in Individual Decision Making", (2005) January/February *IEEE Security & Privacy* 26, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1392696&userType=&tag=1>.

[7] As a recent example, see: P.G. Leon, J. Cranshaw, L.F. Cranor, J. Graves, M. Hastak, B. Ur & G. Xu, "What Do Online Behavioural Advertising Disclosures Communicate to Users?", Carnegie Melon CyLab, CMU-CyLab-12-008, April 2, 2012, <http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf>, the results of this wide-ranging user expectation survey revealed that only a fraction of users were able to identify an industry standard opt-out mechanism was, in fact, an opt out mechanism (many believed it as actually a mechanism for purchasing ads!). This demonstrates the importance of providing clear guidance on the need for privacy defaults or clear obligations on the mechanism of consent.

[8] CIPPIC notes that while it views 'privacy by default' as an element of consent, under the proposed scheme for Convention 108 modernization it may be best positioned as a 'Right of the Data Subject' under Article 8 (not, it should be noted, as an 'additional measure for the controller').

that users *prefer* privacy, as opposed to 'sharing', in contexts where there is a user choice to be made. Another manner in which the 'privacy by effort' problem may be addressed is by providing direct guidance (in the Article itself or in the explanatory note) on the *form* of consent. PIPEDA, for example, expressly ties the form of consent to reasonable user expectations as well as to the sensitivity of the data being processed, given the context in question.[9] This permits for more nuanced and contextual protection for sensitive user data (conversations with friends, movie preferences, reading lists) that respects the contextual integrity of user expectations even in scenarios that fall short of the imperative found in proposed Article 6.

Finally, the proposal in Article 5.2(b), which would exempt data controllers from seeking consent in certain contexts, should not permit data controllers to ignore user consent simply for the purpose of meeting binding contractual obligations. Such obligations are typically within the data controller's power to negotiate and define and, hence, entering into such obligations should not be used as an excuse to bypass what would otherwise be a mandatory consent requirement. Indeed, data controllers could easily enter into such obligations for the sole purpose of bypassing data protection consent requirements. CIPPIC notes that PIPEDA, which puts in place a primarily consent-based data protection regime, has no exception for binding contractual obligations, yet, to our knowledge, this has this has yet to emerge as an obstacle to legitimate business practices.

Article 7 – Data Security

The proposed addition of a data breach notification provision is a welcome addition to Article 7. With data breach notification obligations, care must be taken to strike a careful balance. On the one hand, user notification fatigue should be avoided, so user notification of any and all breaches is not a workable solution. On the other, setting too high and subjective a standard leaves the decision-making process largely in the hands of data controllers subject to strong countervailing incentives militating against disclosure (public embarrassment/loss of organizational reputation; the prospect of costly regulator-imposed security safeguards to remedy the cause of the problem; or even lawsuits resulting from the exposure of user data).[10]

Proposed changes to Article 7 aim to address this issue by adopting a two tier reporting system. A first tier obligates data controllers to report "any violation of data security which may seriously interfere with the right to the protection of personal data" to a competent authority. Tier two, expressed in the explanatory note, adds that where serious risks exist, the data controller should also notify potentially affected data subjects.

The two tier structure adopted by the proposed breach notification regime is effective, but the standards employed should be carefully assessed. Particularly, the first standard should be low enough to ensure that, at minimum, the majority of breaches are reported to a data protection authority. The benefits of an inclusive first tier reporting obligation are several, including: ensuring an objective assessment of whether the breach threatens user privacy, or whether user remedial measures will be necessary (and, hence, user notification should ensue); facilitating evidence-based policy-making with

---

[9] See *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, Schedule 1, Principles 4.3.4 to 4.3.6.

[10] For a comprehensive overview, in the context of an assessment of flaws in a proposed Canadian data breach notification regime, see: J. Lawford & J. Lo, "Data Breaches: Worth Noticing?", December 2011, <http://www.piac.ca/privacy/change_data_breach_bill_to_notify_more_consumers_new_piac_report_1/>.

respect to cyber security by allowing DPAs to track the scope and breadth of the data breach issue; providing strong and necessary incentives for data controllers to adopt strong technical safeguards by assuring their accountability for breaches; ensuring that adequate steps are taken to remedy the underlying factors of a breach. As even low-risk breaches of safeguards can be indicative of more serious security flaws, it is important to ensure an inclusive reporting obligation at the first tier if these objectives are to be fully realized.

The standard employed by the proposed Article 7 amendments – 'may seriously interfere with the right to the protection of personal data' – may not be sufficiently rigorous. By contrast, proposed EU data breach provisions obligate data controllers to report *any* personal data breach (defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed").[11] The EU proposal similarly obligates data controllers to report on the cause of the breach and on steps taken to address it and prevent its recurrence. The Uniform Law Commission of Canada adopted a similar approach (broad 'report to a data protection authority' obligations coupled with the obligation to include details relating to the nature of the breach and steps taken to address it) in its draft data breach notification statute.[12] While U.S. federal data notification proposals do not opt for a two-tier approach, they do obligate data controllers to notify customers of a breach unless there is "no reasonable risk of harm or fraud".[13] The CoE should consider adopting a more rigorous reporting criterion – at least for the lower 'supervising authority' reporting tier.

Finally, it should be specified explicitly (whether in the Article or in the explanatory note) that supervising authorities be given the power to compel data controllers to notify affected customers whenever it is deemed that the second tier reporting standard is met. DPAs in this context serve a function that transcends mere 'reporting' and encompasses oversight. This is critical, as data regimes that leave this assessment in the hands of data controllers are open to subjective organizational decision-making that is likely to favour non-disclosure more often than not.

Article 8 – Rights of the data subject

The proposal adopts a number of new and important user rights that will help citizens protect their privacy in a world that increasingly challenges their capacity to do so. The addition of a user right to information relating to the logic involved in data processing of automated decision-making is especially critical, as is the right to avoid scenarios where automated decision-making can have significant legal implications or other impacts.

---

[11] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data", January 15, 2012, COM(2012) 10 final, 2012/0010(COD), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF>, 'personal data breach' is defined in Article 3, section (9). The obligation to inform a data protection authority is found in proposed Article 28.

[12] Uniform Law Conference of Canada – Civil Section, "Protection of Privacy Amendment Act (Data Breach Notification), Interim Report 2009, <http://www.ulcc.ca/en/poam2/9%20Interim%20Report%20Protection%20of%20Privacy.pdf>. Note that current Canadian legislative initiatives aimed at enacting data breach notification obligations have not yet followed these proposals.

[13] The White House, "Data Breach Notification Legislative Language", May 2011, <http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf>. See also: White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

The absence of a 'droit d'oubliette' is not material. CIPPIC notes that it is not aware that such a right raises free expression concerns (although the means of its enforcement might). Regardless, CIPPIC is of the view that the right to be forgotten overlaps completely with limits on data retention, the right to withdraw consent (which, in turn, is inherent in the right to consent) and the right of opposition. As each of these subsidiary rights is included within Convention 108 or is proposed in this modernization initiative, there remains little reason to adopt a distinct 'droit d'oubliette'.

With respect to the right to opposition proposed in Article 8(d), CIPPIC retains concerns, again, over the proposed standard. Proposed Article 8(d) restricts a citizen's right to refuse consent to a specific data process to scenarios where that citizen can marshal an 'overriding legitimate reason' to object. Consent-based privacy regimes aimed at empowering users to determine how their data will be processed put citizens' subjective preferences at the core of data processing. This is fitting, given that in most contexts users will be interchangeable to data controllers and will be best placed to determine whether a specific process is desirable or not (based on meaningful consent and non-viscous decision-making). In keeping with this theme, users should be able to refuse most data processing activities that are not essential to provision of the service being sought. There should not be a need for 'overriding legitimate reasons' to refuse consent. Rather, data controllers should have 'overriding legitimate reasons' for obligating specific data processing activity.

PIPEDA adopts this stance by preventing organizations from requiring users to consent to non-legitimate purposes as a condition of service.[14] This obligation has proven critical in preventing tied selling and in ensuring the over-arching principle of data minimization, as it prevents organizations from over-collection by means of packaging non-essential processing with essential services in a 'take it or leave it' approach. A clear right of refusal would also be beneficial in addressing scenarios where changes to the character and nature of entire privacy regimes are imposed on an entrenched user base.

Article 9 – Exceptions and Restrictions

Article 9 proposes the adoption of an important and beneficial overarching 'necessary measure in a democratic society' qualifier that limits any exception to the general data protection regime to proportionate measures adopted to address legitimate needs aimed at addressing pressing social needs.

In addition to this over-arching qualifier, the Article 9 exceptions could benefit from greater specificity in articulating specific contexts where an exception might be appropriate. Of greatest concern in this respect is the seeming expansion of section 3 of Article 9, which permits exceptions to elements of the data protection regime undertaken for statistical purposes or for the purposes of scientific research where there is 'no risk of an infringement of the rights and freedoms of data subjects.' The removal of 'personal' from the provision, which now applies only to '~~personal~~ data processing', suggests this provision aims at facilitating statistical and research activities based on anonymized data. If this is the case, it should be state much more explicitly than is currently the case. As currently drafted, the provision suggests the opposite, as non-personal or identifiable data would not be subject to the regime in the first place. Currently, the purpose of this provision appears aimed at facilitating so-called 'big data' benefits while bypassing the need to provide citizens with transparent details regarding such

[14] *Personal Information Protection and Electronic Documents* Act, , S.C. 2000, c. 5, <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>, Schedule 1, Principles 4.3.3: *"An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes."*

practices (Article 7bis), without regard to the sensitivity of the information to be processed (Article 6) and, perhaps most critically, without a right of opposition (Article 8). In place of these critical protections is a more amorphous obligation not to infringe the 'rights and freedoms of data subjects' although, presumably, this obligation already exists. This should be avoided. It is not at all clear that the public benefits of such data processing outweigh the costs in personal privacy. Of greatest concern is the potential inclusion of 'statistical purposes', which is clearly inclusive of commercial analytics and can facilitate a significant amount of online/offline tracking with little clear public benefit.

Second, blanket exceptions in the name of 'public security', 'economic/financial state interests', and 'prevention of criminal conduct', may lead to excessively broad voluntary information disclosures of a type that is not consistent privacy protection in a democratic society. The proposal refers to added clarification that will come in the explanatory report, but in the case of exceptions, it may be better to consider clear and express limits within the scope of the Article itself. As noted in the OECD Privacy Guidelines, exceptions to privacy protection principles, "including those relating to national sovereignty, national security and public policy", should be "as few as possible".[15] As drafted, the proposed amendments would allow data processing for such purposes without regard to the sensitivity of the information (Article 6) and, perhaps most importantly, without the obligation to notify citizens of such processing leads to unauthorized processing (Article 7.2). The latter is critical. Without it, there is no obligation on organizations to notify users or the public of data processing undertaken in the *name* of public security or prevention of criminal conduct, but which is later revealed to have been unauthorized. Finally, it is concerning that data controllers will be permitted to ignore restrictions on retention of citizen data (Article 5.3(d)) in order to facilitate 'public investigations' and in the absence of specific legislative obligations to do so.

Third, the proposed blanket 'freedom of expression' exception raises similar concerns with respect to its scope. It is important to ensure that data protection does not unduly impact on freedom of expression, but it must be kept in mind that in many cases, the parameters of this exception will be determined by organizations without guidance from an objective decision-maker. Private organizations are ill-equipped to make such determinations. The possibility of extending the regime to recognize rights beyond those of 'natural persons' to include those of 'legal persons' (Article 3) is particularly concerning in this context, as it could permit commercial organizations to avoid elements of the data protection regime in the name of 'freedom of expression' even though the expressive value of their commercial expression is low. A more effective approach may be to follow the example in Article 3, which exempts specific private household conduct. Additional contexts that raise specific free expression concerns (such as journalism/news reporting) can be identified.

***** END OF DOCUMENT *****

---

[15] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Council Recommendation, September 23, 1980, <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>, Part One, paragraph 4.

European Magazine Media Association (EMMA) / European Newspaper Publishers' Association (ENPA)

EMMA and ENPA response to proposals from the Council of Europe on the modernization of Convention 108 for the protection of individuals with regard to automatic processing of personal data (5 March 2012)

EMMA, the European Magazine Media Association, and ENPA, the European Newspaper Publishers' Association welcome the opportunity to further comment on the consultation concerning the modernisation of Convention 108.

It is important 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 particular, it is essential when making any changes to the current framework, to take into account the following:

1. A **robust exemption for processing of personal data for journalistic purposes** is crucial to preserve editorial press freedom and safeguard a free and independent, quality press.

2. The possibility for the press to continue to be able to reach out to potential as well as current subscribers via **direct marketing is essential to safeguard press distribution for the consumer as well as the business to business press**, in order to preserve readership, future press subscriptions and media pluralism.

3. The **future of the digital press must not be jeopardized**: publishers have invested substantial resources in developing digital business models in recent years and a **successful future depends on advertising and digital subscriptions, as well as e-commerce**. It is therefore essential that there are no restrictions that will make it difficult for publishers to be able to interact easily with their readers, and adapt to their needs.

We have several specific comments on various new proposed changes to Convention 108:

Article 2 (a): definition of personal data

We have concerns that the proposed additional text to the explanatory report by introducing the aspect of an individual being 'identifiable', would lead to more data than before being considered as 'personal data'. It is unclear as regards what would be "unreasonable time or effort" for identification. The concern is that such a clause could have the result of being unnecessarily burdensome in particular for smaller businesses, so we would propose amending this.

Article 5.2: legitimacy of data processing

The proposed article 5.2 sets out four grounds for legitimate processing of data: "Free specific informed consent (1) or when domestic law provides for: An overriding legitimate interest (2) or is necessary to comply with legal obligations (3) or contractual obligations binding the data subject (4)." Consent is thus one alternative, but not the only one. This is appropriate because it reflects the fact, that there are many different situations where data must be processed. It would make more sense, however, if this proposal was consistent with the six grounds for lawful data processing set out in Article 7 of Directive 95/46/EC.

A press subscription is a product that must be explained, but which has no retail outlet which would allow a publishers' representative, for example, to explain it to a potential customer. In order to safeguard press distribution, direct marketing is therefore crucial. It is therefore vital that any explanation in the Explanatory Report of an overriding legitimate interest makes direct reference to the wording in Article 7 f) of Directive 95/46/CE), i.e., which include "*the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).*"

It is **crucial to keep the possibility to process personal data for the legitimate interests of a third party**. Any attempts to suppress this possibility would result in the end of many titles across the EU dependent on subscriptions sales. For example, in many Member States a large percentage of the subscription circulation of certain newspapers and magazines depends on direct marketing by letters sent to third-party addresses without prior consent, which is permitted by national laws based on Art. 7 (f) and Art.14 Directive 95/46/EC under the condition of information to the addressee and his right to object.

- As regards the **business press**, B2B magazines are often sent to their readers (e.g., doctors, computer and financial specialists etc) based on special address lists of the respective target group for free and without prior consent. This so-called 'controlled circulation' (which can account for up to 90% of the readership of some business titles in some Member States) is necessary to advertise for a subscription of the magazine but also to secure the required reach in order to attract advertisers and therefore to finance the magazine. This would simply not be possible anymore if this form of marketing was not allowed. The benefits to both customers and publishers from this approach can be contrasted with the marginal objection rates to receiving direct marketing by mail without prior consent (e. g. one example cited was less than 10 objections out of 100.000 letters).

- As regards the **consumer press**, figures we have received from individual publishers in the following Member States show that such marketing letters to third party addressees without consent account for the following percentage of subscribers for various publications: Germany (up to 20%); France (up to 40%); Sweden (up to 46%); Portugal (up to 95%); UK (up to 45%).

<u>Article 7bis: Transparency of processing</u>

In order to be able to continue to provide appropriate press distribution, it has to be possible to provide information in a general way. Overly specific requirements where the processing is necessary for the performance of a contract or to conduct pre-contractual measures is in particular not practical for direct marketing activities that take place by mail or by phone, as opposed to online. We have doubts that the provision of all the information required under 7bis (1) (e.g. on an order card, as regularly used for subscriptions), would be possible.

The proposal provides for an obligation to inform on "the preservation period". Nevertheless, in many cases it will not be possible to determine the period of data storing in advance. At the time of conclusion of a subscription for an unlimited period it is difficult to know the length of the subscription period, and thus for how long the personal data has to be stored. Even after the termination of the contractual relationship there might be a legitimate interest to continue using the respective data.

The proposal states that: "*The Explanatory Report will specify (…) any other information necessary to ensure a fair data processing, [which] notably includes information on transfers to other countries. The collection of personal data includes both direct and indirect collection. The information regarding the recipients may also refer to categories of recipients*."

In our view the existence of the word "notably" might create legal uncertainty as regards what type of information a publisher has to provide and would permit an extensive interpretation of the information to be provided.

While we welcome the fact that under Article 7bis (b) a controller shall "*not be required to provide such information where this proves to be impossible or involves disproportionate efforts*", we are concerned that the question of what constitutes impossible or disproportionate efforts will create legal certainty.

It is also unclear when such information would have to be made available.

Right to information (Article 8, a and b)

Under Article 8 a) individuals are entitled on request to obtain "*at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him / her are being* ***processed or not****, the communication of such data in an intelligible form and* ***all available information on the origin of the data and any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7 bis*** ".

This obligation and the corresponding information requirements (as mentioned above) are vague as "reasonable intervals" is not defined and individual companies will not understand how to comply. To avoid resulting in unnecessary expense it would be more appropriate if this information had to be available upon request.

In Article 8 b) it is further determined that the individual should have the right "***to obtain knowledge of the logic involved in the data processing in the case of an automated decision*** ". Given the risk to confidential internal processes it is important that the Explanatory Report notes – as proposed - that, *"the knowledge of the logic involved in the processing cannot be detrimental to legally protected secrets."*

Decision based on automated data processing (Article 8 e)

Under Article 8 e), any person shall be entitled on request "***not to be subject to a decision significantly affecting him / her or producing legal effects concerning him / her, based solely on the grounds of an automated processing of data without having the right to express his / her views***. " We believe that this broad formulation poses a risk to traditional business models.

One problem is that it is not defined when a decision "significantly" affects someone. It is also unclear what is covered by the requirement "based solely on the grounds of an automated processing of data". It cannot be ruled out that this does not include data processing that is essential for publishers, such as measures for so-called interest-based advertising, which is a crucial means of financing digital publishing offers. These provisions could even potentially affect data processing where there is no identification of a specific person, such as where pseudonymous user profiles have been created to avoid identification of the person concerned.

Exceptions and restrictions (Article 9)

Under Article 9 (1) "*no exception to the provisions of this Convention shall be allowed, except to the provisions of Article 5.3, 6, 7.2, and 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to [...] b) protect the data subject or the rights and freedom of others,* ***notably freedom of expression and information*** **".**

We are concerned that the **proposed exception by the Council of Europe does not go far enough in protecting the existing standards for journalistic data processing**. The application of data protection rules to journalistic data processing would make free and independent editorial coverage impossible in many cases, given that a large proportion of all information about politics, economics and other social issues would be covered.

As we highlighted in the introduction to this letter, for editorial freedom of the press a robust exception is needed from general data processing rules in order to allow for the processing of the information collected, storage in the editorial archives and the distribution of the finished articles and publications, including in digital form. Furthermore, this exception must be technology-neutral, covering all distribution channels and media types, and any activity associated with the press.

We would recommend that the **exception must therefore cover at least the articles 4-8, 10-21** to ensure a similar level of protection to now. It should be noted, however, that such an exception does not prevent journalistic activities being covered by national media, libel and privacy laws.

We are also concerned that the requirement that such a derogation "**constitutes a necessary measure in a democratic society" could result in further restrictions.** The suggested text to the Explanatory Report, that "*this provision concerns data processing carried out solely for communicating information to the public, ideas or opinions of general interest, or for literary or artistic expression*" does not help in this regard. We would therefore recommend that this restriction is deleted.

EMMA and ENPA call on the Council of Europe to take on board these comments, given the serious implications of changes to Convention 108 for Europe's press sector.

European Broadcasting Union - EBU

European Broadcasting Union — Union Européenne de Radio-Télévision

Legal Department — *Département juridique*

28.3.2012/2

EBU comments regarding the Council of Europe's new proposals for modernisation of Convention 108

The EBU welcomes the opportunity to provide its comments on the Council of Europe's new proposals to modernise the Convention (T-PD-BUR (2010) 01 Rev_en).

The EBU and its Members are closely following the review process of the data protection legal framework, not only at EU level (i.e. the European Commission draft Regulation replacing Directive 95/46/EC, COM (2012) 11 final, hereafter the "EC draft Regulation") but also with regard to the Council of Europe. Since it is an international, legally binding instrument, the review process of Convention 108 is particularly important.

Certain issues raised in the proposals to modernise the Convention may have an impact on media activities, particularly online, and these include the "freedom of expression and information" exception, the "right to oblivion" (or "right to be forgotten"), data controllers' obligations, and international data transfers.

The EBU warmly welcomes the inclusion of an express reference in the Preamble to the need to reconcile the right to data protection and the right to freedom of expression and an explicit exception for "freedom of expression and information" in Article 9 (1) (b) of the Convention from the requirement of certain provisions. This exception is a key priority for the media.

The EBU notes that the Explanatory Report will contain a broad definition in alignment with the EC draft Regulation, mentioning that the provision concerns data processing carried out "solely for communicating information to the public, ideas or opinions of general interest, or for literary or artistic expression".

As in the EC draft regulation, this exception seems not to be limited to the media as such, but appears also to cover any individual who discloses information, opinions or ideas to the public, which means that, potentially, bloggers and social network users could benefit from the exception, "whenever personal data is accessible to persons outside the personal or domestic sphere".

However, from the media perspective the use of the word "solely" in the Explanatory Report could undermine the purpose of the provision to reconcile data protection and freedom of expression. Information material or data could be held for other purposes coexisting with journalistic and information purposes, such as for investigating a complaint or other regulatory action. Consequently, the word "solely" should be deleted.

As regards the scope of the exceptions from the data protection requirements (i.e. Articles 5.3, 6, 7.2, 7 bis and 8), Article 9.1 ignores other relevant provisions in the Convention where freedom of expression and information is concerned. Additional derogations from certain provisions such as Articles 5.2 (legitimacy of data processing), 8 bis (additional measures for the controller) and 12 bis (supervisory authorities) should be foreseen (as in the EC draft Regulation) when freedom of expression and information is at stake.

The new derogations in Article 9 (2) which are allowed from Article 12, regarding transborder data flows when they are necessary measures to protect freedom of expression and information, are to be welcomed but should be elucidated in the Explanatory Report.

As regards consistency and compatibility with the EU legal framework and the current EC draft Regulation, the EBU welcomes the clarification provided by the Council of Europe on certain issues or concepts which remain unclear in the context of the EC draft Regulation, such as the proposal not to introduce an explicit inclusion of a "right to oblivion" (Article 8) or a "right to be forgotten" and the proposal that the existing provisions (i.e. the right of erasure or rectification of data and the right to object) offer adequate protection.

Introducing a right to be forgotten, as suggested in the EC draft Regulation, could have far-reaching consequences for media online activities even though that right has to be reconciled with freedom of expression and information.

The EBU notes that various proposals are well balanced and proportionate compared to the provisions in the EC draft Regulation with, for example, the express reference to the principle of proportionality in the context of the legitimacy of data processing (Article 5); the reference to "without delay" concerning data breach notification in Article 7 (2); the fact that additional measures (e.g. data protection risk assessment) for the data controller will be adjusted depending on, for instance, the size of the company concerned (Article 8 bis), and the fact that it is for each Party to establish appropriate sanctions and remedies (Article 10).

However, the EBU notes that, contrary to the EC draft Regulation, there is no specific provision in the Council of Europe proposals concerning the processing of the personal data of a child. In general, any provision on protecting the processing of children's data should not prevent the media from engaging with young audiences, and particularly regarding public service content and services which are specially designed for the 16+ age group.

European Multi-channel and Online Trade Association – EMOTA

EMOTA, the European association representing the e-commerce and distance selling sector, is supportive of the approach taken by the Council of Europe in the modernisation of Convention 108, aiming for a technology neutral and principle based proposal. As it is expected that the review of the Convention 108 could be completed before the adoption and implementation of the European Union Regulation on Data Protection, it is key that the text of the Convention allows the fine tuning necessary to reduce legal fragmentation.

In this respect, although the proposal presented by the Council of Europe in March 2012 takes a principle based approach, the mentioning of "explanatory reports", which would be reviewed to complete the text of the Convention for many of the key elements of the Convention (e.g. Article 2, Definitions, Personal Data), could result in an overly descriptive document, which would only increase legal fragmentation due to a possible lack of flexibility.

At the same time, there is a general agreement in the field of data protection that it is time for a broader debate on what are personal data, and what represents the proper consent or proper legal grounds for the processing of personal data in the different scenarios (depending on the effect on the data subject) especially in the context of online activities, both commercial and governmental, as to ensure that the upcoming legal frameworks are future proof and provide legal certainty. We fear that without such a debate, the upcoming legal frameworks would generate confusion due to the incoherent implementation.

Specific comments:

Article 2 – Definition of Personal Data
Although the current text proposes a principle based approach, very much in line with the current European Union Data Protection Directive, the mentioning of an extension of the scope in the "explanatory report", as to clarify the concept of "identifiable", should only refer to the controller's ability to make the data identifiable through reasonable means (*"if identification requires unreasonable time or effort"*). This would prevent the confusion generated by the European Commission Draft Regulation on Data Protection which includes a reference to any other legal or natural third parties.

The proposal to extend the scope of "indefinable" to data which can also "individualise" a data subject could make the Convention too prescriptive and impractical, especially since many of the online services are designed to offer a customized individual user experience. Such an approach could very well lead to a context were all data generated by online activities is considered personal data. The modernisation of the Convention 108 should take into consideration the difficulties in the implementation of the 2009/136/EC "e-Privacy Directive", which were caused by the same approach.

Article 5.b – Compatibility of purposes
EMOTA welcomes the very important reference in Article 5 to the business legitimate interests as a legal ground to process data. The Article also requires the data subject's consent for a change of purpose in the processing of personal data. In this context text makes reference to a list of compatible purposes which would be drafted in an "explanatory report" at a later stage.

EMOTA feels that such a list would be incompatible with the principle based approach and lead to legal fragmentation. The compatibility of purposes for processing should remain a simple issue, established by the controller and processor, under the safeguard of the accountability principle introduced be Article 8 of the Convention.

Article 6 – Processing of sensitive data
We welcome the aim to clarify the concept of "serious risk" in the course of processing sensitive data. However, such clarifications should take account of certain processing procedures which are key to the sale of certain goods and services, where credit checks are necessary, for the safety of both the consumer and the trader (in many countries the offering of a credit to a person in financial difficulty is illegal).

Article 8bis – Additional measures for the controller
The Convention 108 should clearly acknowledge that some measures such as the obligation to appoint a Data Protection Officer, or detailed privacy impact assessments, should be carefully considered in the case of small and medium sized companies, as to not overburden these. This is a very important point which should be harmonised, and included in the text itself, not only in the "explanatory report".

Contact:
Susanne Czech, EMOTA Secretary General
suczech@emota.eu; +32 2 50 02 27

The European Research Federation - EFAMRO / The World Association of Research professional - ESOMAR

We are writing on behalf of EFAMRO, the European Research Federation, and ESOMAR, the World Association of Research Professionals, to comment on the draft revisions to the Council of Europe's Convention 108, recently issued for public consultation. This follows our comments submitted to the Council of Europe during its previous public consultation in March 2011, which are also enclosed for your reference.

We recognise the need to update the Convention in light of technological developments. We support the need to maintain key principles for the automatic processing of personal data.

Council of Europe Recommendation 97(18)

We note the importance for the research sector of Council of Europe Recommendation 97(18) and its Explanatory Memorandum concerning the protection of personal data collected and processed for statistical purposes. This provides a detailed approach for research and provides a reference point for other future Council of Europe recommendations and adopted political texts with regard to processing data for statistical purposes, while recognising the value of market, social and opinion research for democracy, commerce and society. The explanatory memorandum of Recommendation (97)18 covers four important points:

- The importance of treating public and private research equally.
- The distinct character of research: although it is based on individual observations, its objective is not to acquire knowledge of the individuals as such, but to produce synthetic and representative information on the state of a population or of a mass phenomenon. While statistics can frequently take the form of numbers, they can also be non-numerical to allow researchers to establish possible causal links by answering a research question about characteristics of respondents.
- The distinct purpose of research: it is not directed at taking decisions or individual measures, but rather at gathering knowledge of large entities - such as economic cycles, the living conditions of a social group or the structure of a commercial market - as well as at the analysis of phenomena- such as epidemics, opinion trends, fertility or consumer behaviour of households – and therefore arriving at collective judgments or decisions.
- The importance of professional ethics for the sector, including the role of self-regulation.

On the issue of profiling, we remind the Council of Europe of our exchange with the T-PD during the development of Recommendation 2010(13) which recognised that data collected and processed for statistics were already subject to more detailed provisions in Recommendation(97)18.

We recommend that a direct reference to Recommendation 97(18) is inserted into the Convention's Explanatory Memorandum, which would support our recommendations for Article 5 (see below) to explicitly state that processing for research purposes is compatible with the original purpose of processing. This would provide a direct link to help the Council of Europe and the Member States in future understand the importance of protection of personal data for research.

Aligning Convention 108 and the EU Data Protection Framework

Before commenting on the articles, we would like to note the importance of aligning the language and provisions addressing research in both Convention 108 and EU law.

- In particular, the current EU Directive 95/46/EC, as well as the recent proposal for a General Data Protection Regulation (published by the European Commission on 25 January 2012) contain certain conditions for **historical, statistical and scientific** research These have their origin in Article 9 paragraph 3 of Convention 108. These provisions allow access to data to compile research and statistical records which in turn inform better and more accurate assessment of, and decision making on, important economic and social activities in Europe. These arrangements have worked successfully since the introduction of Directive 95/46/EC

  and we ask the Council of Europe to take a complementary approach in the Convention to provide legal certainty and continuity.

- The Convention should also recognise the value of private and public research similar to recital 126 in the proposed Regulation. Large scale social research projects are simply not possible without the resources and expertise of private organisations.

- Directive 95/46/EC and the proposed Regulation both provide an exhaustive list of types of data in the category of sensitive personal data (special categories of personal data). We strongly encourage the Council of Europe to take a complementary approach to the EU, ensuring legal certainty by avoiding a non-exhaustive list of types of data considered sensitive.

The articles that we wish to comment on in particular are Article 5 and Article 9:

Article 5 - Quality of data and legitimacy of data processing:

With particular regard to paragraph 3(b) of this article, we note that a provisional note has been added to reserve a space in the Explanatory Memorandum for giving examples of compatible purposes and that processing for statistics, historical or scientific research purposes is *a priori* compatible provided that other safeguards are ensured.

We strongly encourage the Council of Europe to consider including this declaration of *a priori* compatibility of statistical or scientific research in the text of Article 5 to avoid any misunderstanding among Member States when applying the Convention in practice.

The 5 March public consultation text from the Council of Europe also creates a condition that research can be *a priori* compatible with the original process 'provided that other safeguards exist and that the processing is not the ground for a decision to be taken concerning the data subject'. This additional phrase is confusing and unhelpful. Research, by definition, never involves the taking of decisions concerning individuals.

We refer the Council of Europe to the Recommendation 97 (18) which clearly states in section 1, definition of 'statistical purposes' that 'such operations exclude any use of the information obtained for decisions or measures concerning a particular individual'.

We recommend that the Council of Europe avoid blurring the distinction of research with other forms of processing such as marketing, which do involve direction action or decisions in regard to

individuals. If there is a separate purpose that the Consultative Committee has in mind, it should make clear that this is not the same as statistical research.

Article 9, exceptions and restrictions:

In the 5 March public consultation text, a set of brackets have been placed around the words 'statistical purposes or for' in Article 9 paragraph 3, suggesting their potential removal. We strongly support maintaining this text in the Convention, to ensure that it aligns with the provisions for historical, statistical and scientific research in the EU, providing continued legal certainty in this area for researchers

Regarding Article 9, paragraph 1(b), we support permitting Member States to impose restrictions on the exercise of rights in specified articles of the Convention with respect to data processing carried out solely for communication of public information, ideas or opinions of general interest. This is particularly important for the publication of research/opinion poll results in the media, notably for political opinion polling.

On a right to be forgotten *(although this right is not mentioned in the proposals for revision currently):* If such a right is considered by Member States in the coming months, EFAMRO and ESOMAR wish to remind the Council of Europe of the exemption from this right for research in the EU. As noted by Crispin Blunt, representative of the UK at the Council of Europe panel at the CPDP conference on 27 January 2012, the proposed Regulation provides that the right to be forgotten would not be applied to research, as is the case in Directive 95/46/EC, Article 12. Moreover, the right does not apply in the context of anonymous data.

EFAMRO and ESOMAR wish to remain in close contact with the Council of Europe in the coming months as the Convention text goes through further revisions and while the Explanatory Memorandum is drafted, with particular interest in provisions relating to recognition of historical, statistical and scientific research as a compatible purpose with the original automatic processing personal data.

We remain at your disposal for any further information that you or the Members of the T-PD may require and would welcome to participate in further stakeholder consultations or hearings as appropriate. e.g. the stakeholder hearings in early May if these are still going ahead as planned.

With regard to Recommendation 97(18), we understand that the Council of Europe is considering whether to revise this and in this context, we would like to follow up our points made in this letter

individuals. If there is a separate purpose that the Consultative Committee has in mind, it should make clear that this is not the same as statistical research.

FEDERATION OF EUROPEAN DIRECT AND INTERACTIV MARKETING
(Mathilde Figuet – EU Legal Afffairs Adviser)

FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING

PUBLIC AFFAIRS & SELF-REGULATION 30 March, 2012

FEDMA submission on the proposal for the modernisation of Convention 108

FEDMA (Federation of European Direct and Interactive Marketing Associations) would like to take this opportunity to respond to the Council of Europe's proposal for the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data.

General Comments:
FEDMA welcomes the Council of Europe's work on modernising Convention 108 on data protection, providing a comprehensive framework equipped to handle privacy issues resulting from technological developments, and ensuring enforcement of data protection standards within the jurisdictions of the Convention.

FEDMA supports the basic principles of the Convention, and especially appreciates that the Convention protects individuals against privacy intrusions not only by the private sector, but also by public authorities. FEDMA believes that 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.

However, FEDMA is concerned about some provisions of the Convention 108.

Article 5:

- Purpose limitation

Article 5. b states that personal data may not be further processed in a manner that is incompatible with the purposes for which they were originally collected, except when the processing is provided for by law, or the data subject has given its consent. FEDMA strongly believes that in assessing compatible use of data, the purpose for which the data were originally obtained should be assessed against the new intended purpose of the processing. Only when there is no resemblance between these purposes, should the legal grounds for legitimate interest of the data controller be taken into account.

Article 6:

- Special categories of data

Article 6 no longer includes an exhaustive list of special categories of data. Rather it states that all personal data presenting serious risks to the rights and interests of the data subject can be classified as falling under "special category of data". The explanatory memorandum further defines serious risks as risks of injuring dignity or physical integrity.

FEDMA strongly disagrees with this proposal, as it will lead to legal uncertainty for industry and governments alike. The categories of personal data deserving 'special protection', are very much individually and culturally determined. Furthermore, harmless data when applied in a different context can be considered as presenting serious risks to data subjects. Age, or year of birth, is generally considered harmless[1]. However, when used in a different context, can become more of a personal issue as when selecting recipients for promoting hearing aids,. A 60 year old, who likes to be seen as being younger than his/her age, may feel offended (i.e. his dignity injured) be receiving such advertisement. The perception what is sensitive data varies depending of the person and the context of processing.

Same data present different level of risk depending on the national and cultural background. In the southern European States 'membership of a trade union' is more an issue then in the northern states.

FEDMA therefore strongly urges the Council to explicitly state what data are considered special categories of data in an exhaustive list.

Article 8:

- Automated decisions

The proposal introduces in article 8. e the right of the data subject not to be subject to a decision based solely on the grounds of automated processing without having the right to expose his/ her views. FEDMA believes that this right should be limited. An individual should have such a right when the decision-making process has negative legal effects on him/her.

When an individual for example wants to retract money from an ATM machine and the machine refuses, this is an automated decision solely based on the fact that the data subject doesn't have enough credit (contractual agreement). In this case, the individual should not have the right to expose his views. The Convention should recognize that automated decisions are a fundamental part of commercial, governmental, ideal and charitable business processes and are essential for the functioning of the internal market. Only when the interests pursued by the controller are overridden by the interests for fundamental rights and freedoms of the individual, should the individual have the right not to be subject to an automated decision without having exposed his views.

Article 8 bis:

- Additional measures for the controller

Article 8 bis introduces additional measures of accountability for the data controller, such as a privacy risk analysis and other documentation on processing. However, we feel that the article is too prescriptive, and places too much emphasis on documentation. The

[1] In German Data protection law, year of birth belongs to the so called 'List Data' that are by nature considered non-intrusive. (BDSG Article 28 Paragraph 3 2nd sentence)

problem of being prescriptive is the lack of flexibility. There is no one-size-fits-all model, as measures to be put in place for data protection depend on multiple factors such as the size of a database, whether or not data will be disclosed to third party, type of data, type of processing, just to name a few. Moreover, the importance placed on documentation leads to unnecessary administrative burden. Just for maintaining sets of documents that prove the organisation's data protection efforts, many mid to large organisations would need to dedicate a person/department to fulfil these duties. This investment could have contributed to the protection of the right to data privacy far better, when it could be spent on, for instance, privacy awareness education for employees and data subjects. FEDMA therefore strongly recommends the Council to suggest clauses stating the principles, which will in turn provide the data controller with the freedom to choose his own means to ensure data protection within his organisation, as well as preventing paperwork for the sake of paperwork.

INSURANCE EUROPE *(William Vidonja – head if Single market & Social Affairs)*

Introductory remarks

Insurance Europe (former CEA), the European insurance and reinsurance federation, welcomes the opportunity to contribute to this second consultation on the Modernisation of Convention 108, launched by the Council of Europe (CoE).

Insurance Europe participated in the first CoE consultation last year and is content to see that some of its concerns raised previously have been taken into consideration by the T-PD committee. This being said, Insurance Europe would like to comment on the following points of the new proposals on the Modernisation of the Convention 108.

Insurance Europe notes that EC Directive 95/45 on data protection is currently under revision and hopes there will be no significant discrepancies between the future modernised CoE Convention 108 and the future EU regulation and directive.

Article 5 – Legitimacy of data processing and quality of data

- *Par.1 "Data processing shall be **proportionate** in relation to the purpose pursued and reflect a fair balance between the public or private interests, rights and freedoms at stake".*

Insurance Europe highlights that this paragraph contradicts the existing principles of the legitimacy of data processing as it is given in Article 5 par.2 (*processing of personal data by consent)*. Where the processing of personal data is based on other legal grounds such as national law or a contract, there is no need for an additional examination of proportionality.

It should also be noted that the existing EU legislation requires the insurance industry to collect certain data in order to carry out its business. For example anti-money laundering (AML) legislation requires insurers to verify the accuracy of certain personal data, eg the identity of the policyholder/beneficiary, the origin or the destination of the funds. It is vital that the interpretation and application of these new provisions do not hinder the fulfilment of existing regulatory requirements imposed on insurers.

Moreover, as part of anti-fraud measures, insurers need to collect, process and share certain relevant data. We support measures that ensure appropriate consumer protection, however the legislative framework must recognise the need for organisations to share information for such purposes.

Detecting fraud protects honest consumers. It is important that efforts to combat fraud (which are in the overriding interests of individual consumers and of society as a whole) are supported and explicitly recognised in the development and application of the law rather than being restricted.

Furthermore, as part of the underwriting process, insurance companies need comprehensive information and data about the risk to be insured. Being able to access, process and store relevant personal data is central to insurers' ability to provide consumers with appropriate products at fair prices.

- *Par.2a) "Each Party shall provide that data processing can be carried out only if the data subject has **freely given his/her specific and informed consent**"*

There should be clarity as to the type of consent required and this should not be unnecessarily burdensome for organisations and consumers.

To perform its activities, the insurance industry needs clarity on how the aforementioned conditions can be met. The word *specific* in the provision on consent introduces a layer of uncertainty. Moreover, when a data subject gives its *consent* in an insurance context, this *consent* is given for both the scope and the consequences of the data processing.

For this reason Insurance Europe propose the deletion of the word *specific*. However, if the CoE decides to maintain that the consent has to be *specific*, Insurance Europe would then suggest that the word *specific* is interpreted as *intelligible* in line with the Opinion 15/2011[1] of the Article 29 Working Party.

Finally, if the data subject's right to withdraw his/her consent is included in the Explanatory Report, there should be an exemption for cases where the withdrawal would contradict good faith, create legal hindrances to the fulfilment of a contract, contradict regulatory requirements, or prevent or restrict anti-fraud measures.

1 – *opinion 15/2011 on the definition of content*

Article 6 – Processing of sensitive data

- *"Personal data may not be processed for the racial origin, political opinions or religious or other beliefs that they reveal. Nor may genetic data, data concerning health or sexual life, biometric data, personal data relating to criminal convictions, as well as personal data recognised by a Party as presenting a serious risk to the rights and interests of the data subject, in particular a risk of unlawful discrimination, be processed.*

  Such data may nevertheless be processed where domestic law provides appropriate safeguards."

If the Consultative Committee includes genetic or biometric data in the "special category of data", then it must be ensured that characteristics such as gender and age, which are visible to everyone, and also family history, are not part of them. Otherwise the definition will be incompatible with the provisions of other pieces of national or European legislation, such as the proposed EC general data protection regulation.

Insurance Europe would like to underline that the Explanatory Report includes a broad definition of *genetic data*, ie *characteristics acquired during early prenatal development* which are not in fact caused by genetic conditions but by external conditions such as lack of oxygen. Insurance Europe suggests that the *biometric data* definition should be restricted to biometric detection data, otherwise data on physical attributes needed for the actuarial mathematics will fall under it, creating problems for the insurers.

According to article 6 sensitive data may nevertheless be processed where domestic law provides appropriate safeguards. This means that the processing of health data could be simply and merely forbidden if domestic law does not provide any. This proposal seems to go far further than the EC proposal for a regulation which allows several exceptions like the consent of the data subject.

Article 7 – Data Security

- 2. *"Each Party shall provide that the controller shall notify, without delay, at least the supervisory authorities within the meaning of Article 12 bis of this Convention of any violation of data security which may seriously interfere with the right to the protection of personal data.*

The Explanatory Report will add that the controller should also ***notify the data subjects*** *in case of serious risks.*

Insurance Europe welcomes the CoE approach on data security and agrees that the supervisory authorities and data subjects should be notified only about breaches that pose a significant risk of harming data subjects.

If the data subject is notified for every breach of data, ie those posing significant risk and others that do not, important notifications might be overlooked, leading also to consumers' apathy.

Moreover, in order to ensure the right understanding of *seriously interfere*, Insurance Europe suggests that the explanatory note of the Report of the 24th Meeting of the Bureau of the Consultative Committee (28-30 June 2011) should be added to the Explanatory note on the Convention, highlighting that the obligation to report security breaches should not become trivial and should only concern breaches related to a certain volume of data.

Insurance Europe would like to underline that insurance companies and other financial institutions have to notify the data breaches only to supervisory Authorities within the meaning of Article 12 bis of the Convention and to sectorial supervisory Authorities.

Article 8 – Rights of the data subject

- *a) Any person shall be entitled on request to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him/her are being processed or not, the communication of such data in an intelligible form and all available information on the origin of the data and any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis.*

  b) To obtain knowledge of the logic involved in the data processing in the case of an automated decision.

  The Explanatory Report will explain that the knowledge of the logic involved in the processing cannot be detrimental to legally protected secrets.

Insurance Europe 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 the data are disclosed repeatedly and where it is difficult for the data subject to identify the body which originally collected the data.

Careful consideration must be given not to introduce any requirement to disclose information while such disclosure could be in breach of competition law. In the case of the insurance industry, the legislative framework must not make it possible for insurers to reveal their underwriting criteria or processes to other insurers as this would be in breach of competition law. Insurance Europe would therefore propose the deletion of Article 8b.

Insurance Europe is the European insurance and reinsurance federation. Through its 34 member bodies — the national insurance associations — Insurance Europe represents all types of insurance and reinsurance undertakings, eg pan-European companies, monoliners, mutuals and SMEs. Insurance Europe, which is based in Brussels, 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 100bn, employ nearly one million people and invest almost €7 500bn in the economy.

www.insuranceeurope.eu

INTERNATIONAL ASSOCIATION OF IT LAWYERS

The following have submitted their comments on the text of the Convention 108 proposal:

- **Prof. Sylvia Kierkegaard,** University of Southampton and president of the International Association of IT Lawyers.
- **Dr. Elisabeth Thole,** Attorney at Van Doorne N.V. (Netherlands).
- **Joseph V. DeMarco,** Partner and Attorney at DeVore & DeMarco (NY) and member of the Professional Board of Computer Law and Security Review

26 March, 2012.

Introduction

The Draft Proposal on the Modernization of Convention 108 is the result of the public consultation in spring of 2011. The latest modernization proposal was reviewed on the basis of the 27th plenary meeting of the Consultative Committee of the Convention (from 29 November to 2 December 2012) and the 26th meeting of its Bureau (from 6 to 8 February 2012).
The proposal deals with new data protection challenges for privacy resulting from the use of new ICTs and reaffirms the Convention's potential as a universal standard and its open character. The Convention remains the only legally-binding standard which has the potential to be applied worldwide. The proposal for modernisation of the Convention seems to be inspired by the EU Data Protection Directive 95/46. This same Directive is currently under revision itself. It may be advisable to await the definite outcome of that revision for the purpose of modernisation of the Convention. Furthermore although the preamble (11) of Directive 95/46 does refer to the Convention, the relation and ranking order between the Convention and EU regulatory instruments on the subject should (also) be stipulated in the revised Convention itself.
This Submission endorses the text of the proposals set out in 'Modernisation of Convention 108 – New Proposals' (T-PD, March 2012) except for the following specific texts and comments in our Submission. 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. Our input has as starting point that data protection is very important. However legislation should not impose unnecessary burdens on businesses without effectively resulting in additional protection. Privacy and business interests need to be balanced.

CONVENTION PROPOSALS	Submission
Preamble Considering that it is necessary to guarantee the protection of fundamental rights and freedoms, as well as everyone's dignity, in particular through the right to control one's own data, taking into account of the intensification of processing and exchange of personal data ;	Preamble Considering that it is necessary to guarantee the protection of fundamental rights and freedoms and everyone's dignity, in particular through the right to control one's own data, taking into account of the intensification of processing , exchange **and storage** of personal data ; *Explanation: The right to control one's data*

	includes also the right to control the retention and storage of his personal data.
Chapter 1 General Provisions Article 1- Object and Purpose The purpose of this Convention is to secure for every individual, subject to the jurisdiction of the Parties, whatever their nationality or residence, the right to the protection of personal data, thus ensuring the respect for their rights and fundamental freedoms and in particular their right to privacy , with regard to the processing of their personal data.	Chapter 1 General Provisions Article 1- Object and Purpose The purpose of this Convention is to secure for every individual, subject to the jurisdiction of the Parties, whatever **his** nationality or residence, the right to the protection of **his** personal data, thus ensuring the respect for **his** rights and fundamental freedoms and in particular **his** right to privacy , with regard to the processing of **his** personal data. *Explanation: The word " Individual" is in singular form and therefore "his" should be used instead of the word "their".* Comments *The concept of individuals subject to Parties' jurisdiction may lead to confusion here. A State can for example have jurisdiction over its citizens when they're abroad. States must also protect the data of those citizens? Such protection may be impossible to effectuate in practice and would also result in legal uncertainty for data controllers (who in the online world generally do know where someone is situated, but not its nationality). Consequently, we would suggest in this case adhering to the territory concept in this context.*
Article 2 -Definitions A. unchanged Make an addition to the Explanatory Report, specifying in particular that an individual is not considered "identifiable" if identification requires unreasonable time or effort for a person who would be informed of it.	Article 2 -Definitions A. unchanged Make an addition to the Explanatory Report , specifying in particular that an individual is not considered "identifiable" if identification requires unreasonable time, **cost or manpower effort** for a person who would be informed of it. **The determination of the reasonableness of time and effort must be determined relative to the privacy interests which may be adversely affected or other factors surrounding facts and circumstances ,such as economic costs.**
Article 2 - Definitions c. "data processing" means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of	Article 2- Definitions c. "data processing" means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, preservation, alteration, retrieval, disclosure, making available, **transfer,** erasure or destruction

logical and/or arithmetical operations on data; where no automated processing is carried out, data processing means the operation carried out on personal data within a set of structure which allows to search the data related to a specific subject:	of data, or the carrying out of logical and/or arithmetical operations on data; where no automated processing is carried out, data processing means the operation carried out on personal data within a set of structure which allows **search of the data** related to a specific subject; Comments: *The introduction to the proposal of 5 March 2012 refers to the incorporation of a new definition of "service provider". Such new definition is not present in the proposal; instead a definition of processor is included. We agree with that last definition, but suggest clarifying whether a definition of "service provider" will (also) need to be taken into account or not.*
Article 3 :Scope Each Party undertakes to apply this Convention to data processing carried out by any **controller subject to its jurisdiction**.	Article 3 :Scope Each Party undertakes to apply this Convention to data processing carried out by any controller subject to its jurisdiction. Comments *We encourage specifying that each Party must ensure that a controller is subject to its jurisdiction if it (i) offers goods or services to data subjects on the Parties' territory; or (ii) monitors those data subjects' behavior, in line with the proposed EU Data Protection Regulation.*
Article 3 :Scope *In the explanatory report, specify what is meant by exercise of purely personal or household activities, and making accessible to persons outside the personal or household sphere.* *Specify that while the processing concerns data of natural persons, the Parties nevertheless have the possibility to extend the protection to legal persons.*	Article 3 :Scope *In the explanatory report, specify what is meant by exercise of purely personal or household activities, and making accessible to persons outside the personal or household sphere.* *Specify that while the processing concerns data of natural persons, the Parties nevertheless have the possibility to extend the protection to legal persons.* Comments *The line between the two can, as all seem to recognize, be quite blurry. Blogging, tweeting, and the use of social networks often involve situations where purely personal conduct bleeds into non-personal. Perhaps consider examples such as the ones listed in this note.*
Article 5 Legitimacy of data processing and quality of data 2. Each Party shall provide that data processing can be carried out only if:	Article 5 Legitimacy of data processing and quality of data 2. Each Party shall provide that data processing can be carried out only if:

a) the data subject has freely give his/her specific and informed consent b). it is provided for by domestic law for an overriding legitimate interest or is necessary to comply with legal obligations or contractual obligations binding the data subject;	a) the data subject has freely give his/her specific , **explicit** and informed consent b). it is provided for by domestic law for an overriding legitimate interest or is necessary to comply with legal obligations or contractual obligations binding the data subject; *Explanation: Because there is now a lot of invalid consent on the Internet, an explicit consent is necessary to enforce user's control of his data.* **Comments:** *This section 2 of article 5 seems to be inspired by article 7 of the EU Directive 95/46, but only includes part of the legitimate grounds mentioned in that article. We recommend fully following either article 7 of the Directive, or - preferably - the relevant article in the Data Protection Regulation (article 6 in the proposal).*
Article 5 Legitimacy of data processing and quality of data 3. Personal data undergoing processing shall be : a) processed fairly and lawfully; b) collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes unless the data subject has given his/her explicit consent or it is provided for by domestic law; The *Explanatory Report will give examples of compatible purposes (statistics, historical or scientific research purposes that are a priori compatible provided that other safeguards exist and that the processing is not the ground for a decision to be taken concerning the data subject).* c) adequate, relevant and not excessive in relation to the purposes ,for which they are processed; d) preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed;	Article 5 Legitimacy of data processing and quality of data 3. Personal data undergoing processing shall be : a) **obtained** and processed fairly , lawfully **and limited to a strict minimum** ; b) collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes unless the data subject has given his/her explicit consent or it is provided for by domestic law; Comments: "The *Explanatory Report* is not clear on what "other safeguards" means here. Is it technical safeguards such as, for example, encryption, or policy, administrative, physical or regulatory safeguards? c) adequate, relevant and not excessive in relation to the purposes ,for which they are processed and **stored** ; d) preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed and **stored** ;
Article 7 – Data Security 2. Each Party shall provide that the controller shall notify, without delay , at least the supervisory	Article 7- Data Security 2. Each Party shall provide that the controller shall notify, without delay , at least the supervisory

authorities within the meaning of Article 12 bis of this Convention of any violation of data security which may seriously interfere with the right to the protection of personal data.	authorities within the meaning of Article 12 bis of this Convention of any violation of data security which may seriously interfere with the right to the protection of personal data. **(a) Violation of data security which interferes with the right to protection of personal data is deemed to be serious when it poses a significant risk of financial, reputational, physical ham, significant humiliations or other harm to the individual. When the use or disclosure of protected health information does not include the identifiers, such as date of birth, and zip code, it does not compromise the security or privacy of the protected health information.** **(b) The notification to the supervisory authorities shall describe the consequences of, and the measures proposed or taken by the provider to address the violation of the data security.** **3. Each Party shall provide that the controller shall notify, without delay , the subscriber or individual of any violation of data security which may seriously interfere with his right to the protection of personal data.** **(a)The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the violation of data security.** *The Explanatory Report should state that a reasonable delay is one of 7 days or more, unless the Controller seeking additional time demonstrates that such time is reasonably necessary under a multi-factor standard.*
Article 6 Processing of sensitive data *The Explanatory Report will explain that "serious risk" includes injury to dignity or to physical integrity, "genetic data… means all data concerning the hereditary characteristics of an individual or characteristics acquired during early prenatal development, "biometric data… means all data concerning the physical, biological of physiological characteristics of an individual that allow his/her unique identification.*	Article 6 Processing of sensitive data Comments: *Does injury to dignity encompass economic harm to the subject?* *Does this include emotional or behavioral characteristics, as emotional detection software exists?*

Article 8 Rights of the data subject The controller must design data processing operations in such a way as to minimise the risk of interference with the right to the protection of personal data. *The Explanatory Report will also specify that Parties may adjust these requirements on the basis of company size, volume of data processed, risks involved, etc.*	Article 8 Rights of the data subject The controller must design data processing operations in such a way as to minimise the risk of interference with the right to the protection of personal data. Comments *The Explanatory Note should address concrete factors for inclusion into the analysis as to whether a risk analysis meets appropriate standards. Perhaps consider some of the factors outlined in the "Safeguards Rule" of the Gramm Leach Bliley Act.* *At a minimum, such a risk assessment should include consideration of risks in each relevant area of [the financial institution's] operations, including:* *a. Employee training and management;* *b. Information systems, including network and software design, as well as information on processing, storage, transmission, and disposal; and* *c. Detecting, preventing, and responding to attacks, intrusions, or other system failures.* *For example, an institution must first disclose its privacy policy to consumers and allows them to "opt out" of that disclosure.* *Is it legitimate to consider the cost to benefit ratio or the sensitivity of the data in question? If so, perhaps the Explanatory Note should add it as additional examples.*
Article 9 Exceptions and restrictions 2 (a) protect State security, public security, the economic and financial interests of the State or the prevention and suppression of criminal offences;	Article 9 Exceptions and restrictions 2 (a) protect State security, public security, the economic and financial interests of the State or the prevention and suppression of criminal or **tortuous** offences;
Article 10 "Sanctions and remedies " Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter	Art. 10 Sanctions and Remedies Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter. a) **Each Party shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the domestic law applicable to the processing in question.** b) **Each Party shall provide that any person who has suffered damage as a**

	result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Convention is entitled to receive appropriate compensation from the controller for the damage suffered. **Comments:** *It may be useful here to specify the concept of damage in this context. Furthermore establishment of an enforcement mechanism towards the Parties (countries) may be advisable.*
Article 12 - Transborder flows of personal data and domestic law 4. Notwithstanding paragraphs 2 and 3 , each Party may provide that the disclosure or making available of data may take place without the law applicable to the recipient ensuring, for the purposes of this Convention, an adequate level of protection of data subjects, if: a) the data subject has given his/her consent, after being informed of risks due to the absence of appropriate safeguards, or b) the specific interests of the data subject require it in the particular case, or c) legitimate interests, in particular important public interests, prevail.	Article 12 - Transborder flows of personal data and domestic law 4. Notwithstanding paragraphs 2 and 3 , each Party may provide that the disclosure or making available of data may take place without the law applicable to the recipient ensuring, for the purposes of this Convention, an adequate level of protection of data subjects, if: a) the data subject has given his/her **explicit** consent, after being informed of risks due to the absence of appropriate safeguards, or b) the specific interests of the data subject require it in the particular case, or c) legitimate interests, in particular important public interests, prevail. **Comments**: *Not all countries Party to the current Convention are deemed to provide adequate protection under EU law. It should be clarified how this proposed article relates to the adequacy decisions of the European Commission based on article 25 of Directive 95/46 (see also article 41 of the proposed General Data Protection Regulation 2012/001).*
Article 18 Composition of the committee A Consultative Committee shall be set up after the entry into force of this Convention. 3 The Consultative Committee may, by a decision taken by a majority of two-thirds of its representatives [voting] [entitled to vote], invite an observer to be represented at its meetings.	Article 18 Composition of the committee A Consultative Committee shall be set up after the entry into force of this Convention. 3 The Consultative Committee may, by a decision taken by a majority of two-thirds of its representatives **voting**, invite an observer to be represented at its meetings.

ALTERNATIVE PROPOSALS: The Alternative Proposals are unnecessary.

SAFRAN MORPHO

Nous sommes étonnés de constater que cette version de la dernière proposition de texte considère les données biométriques comme des données sensibles.
Cette évolution qui étend la définition des données sensibles aux données biométriques a priori sans prendre en compte les circonstances du traitement des données nous apparait un peu excessive.
En effet, il nous semble qu'une approche circonstanciée serait plus appropriée pour prendre en compte les risques potentiels, plutôt que considérer ces données comme sensibles par nature.
Morpho, en tant qu'acteur majeur de solutions d'identification et d'application de gestion des droits des personnes utilisant la biométrie, craint qu'une telle posture ne conduise à déstabiliser l'industrie européenne dans ce domaine face à la concurrence mondiale, et ne menace à terme sa pérennité.
La protection des données est au cœur de nos travaux de recherche, elle est prise en compte dans le développement de nos produits et solutions, et nous travaillons conjointement en étroite collaboration avec la CNIL.
Dans ce contexte, nous vous adressons de nouveau le document que nous vous avions adressé le 10 mars 2011, et souhaiterions rencontrer les personnes chargées de la rédaction du texte afin de leur expliquer plus en détail, les raisons pour lesquelles une approche plus souple concernant l'encadrement juridique des données biométriques serait souhaitable.

SAFRAN
Morpho

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.

SAFRAN
Morpho

<u>Question 11</u> : 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.

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

University of Kassel-Germany *(Matthias Pocs)*

My impression is that the consultative committee proposed a solid and modern text.

Please allow me to draw attention to one of the modern instruments involved and an addition to the definition of controller. Article 8bis provides for the accountability principle including privacy impact assessment and privacy by design. In addition to my suggestion of changing wording ("impact assessment"), I would like to stress the new competence proposed in Article 23 of the EU Data Protection Regulation. Accordingly the EU Commission can adopt technical standards proposed by a committee (consisting of Member States' experts). This amendment is noteworthy because technology design is determined by global players and standardisation organisations mainly from the US. In order to give weight to European values in technology design, the recognition of technical standards by European legislators are crucial.

Can the consultative committee support this ambitious approach of European legislators recognising certain technology design goals?

Such design goals are primarily aimed at minimising personal data by means of anonymisation and pseudonymisation techniques. Whereas anonymisation is preferable, personal data are also necessary to the controller. Therefore human rights protection can also be achieved by a certain kind of pseudonymisation involving a trusted third party - an "informational clearinghouse." This brings me to my second suggestion. For promoting such design approaches the EU Commission's proposal of "joint controllership" in Article 24 of the EU Data Protection Regulation seems to be useful. Accordingly the original controllers can delegate the data protection compliance to the "informational clearinghouse." This is an incentive for authorities and companies to use such minimum-risk solutions since they would be relieved of bureaucratic duties.

Therefore I suggest to include a provision for joint controllership for which the Convention Proposal paved the way in the definition of controller (*"jointly with others has the decisionmaking power with respect to data processing"*).

I am at your disposal for further comments (for elaboration of these ideas please see publication in full text at www.matthiaspocs.de).

University of Oxford – Centre of Socio-Legal Studies (CSLS)
(David Erdos - Katzenbach Research Fellow)

I am writing in relation to proposals made by the Bureau in relation to the modernization of Convention 108. I would particularly like to acknowledge all the hard work which the Bureau has obviously put in to this process and the many important and useful changes it now suggests. Particularly positive is the great expansion of scope of exemptions specifically in favour of "scientific research" current set out as a potential new Article 9.4 and also the specific inclusion of also wide-ranging exemptions in favour of public freedom of expression included in proposed Article 9.3.

The need for clarification of the relationship between the research and freedom of expression provisions

My concern in writing this short submission is to ensure that the relationship between these two clauses is clarified. This is important because Article 9.4 only applies when "there is obviously no risk of an infringement of the privacy of the data subjects". This is a very opaque and potentially highly restrictive phrase which as currently included in the existing Convention 108 has encouraged Member States to adopt numerous restrictions on the use of the research exemption including, for example, full anonymization and/or licensing by the Data Protection Authority. Whilst some of these restrictions and the general language of Article 9.3 may be appropriate for research intended purely for a private benefit (e.g. certain types of commercial research), they are not appropriate for "research" by academics in the social sciences and humanities which is intended to result in the dissemination to the public of new knowledge and insights. Investigatory work by academics in this area may not be intrinsically different from that of the preparatory work of independent writers and journalists writing on topics of public interest. Moreover, in order to further publically important knowledge and understanding such work on occasion necessarily have to be covert (e.g. to unearth police corruption), identifiable (especially in contemporary history work) and, at least as regards publicly accountable behaviour, may even cause an element of warranted damage or distress (e.g. a study uncovering the true activities of an alleged genocide perpetrator). It is therefore very important that the text of the Convention or failing that the explanatory memorandum makes clear that the fact that something may be designated "research" under Article 9.3 does not preclude it from benefiting from potentially more liberal provisions under Article 9.4 so long as the work in question meets the tests of being orientated towards "communication of public information, ideas or opinions of general interest, or for literary or artistic expression, when such restrictions are necessary to reconcile the right to private life and the freedom of expression and information". In this regard it is also important the word "solely" in Article 9.4 does as exclude such a result. Given that it may be so interpreted it seems that a rephrasing here should be made.

Further information

The recently organized "Threats to the University" Conference at the University of Cambridge resulted in the issuing of a statement stressing the need to ensure that academic work benefited on an equal basis to freedom of expression as others. This statement (which I was involved in drafting) can be read here: http://www.cpl.law.cam.ac.uk/threats_to_the_university/conference_statement_regarding_data_protection.pdf. I am also author of a number of articles which have explored in much greater detail the case for such equal treatment which you might find useful. These are:

- "Freedom of Expression Turned On Its Head: Academic Social Research and Journalism in the European Union's Privacy Framework" (forthcoming in *Public Law*)

- "Constructing the Labyrinth: The impact of data protection on the development of 'ethical' regulation in social science" (*Information Communication and Society*, Vol. 15 (1), pp. 104-123 (2012))
- "Systematically Handicapped? Social Research in the Data Protection Framework", *Information and Communications Technology Law*, Vol. 20 (2), pp. 83-101 (2011)
- "Stuck in the Thicket? Social Research under the First Data Protection Principle", *International Journal of Law and Information Technology*, Vol. 19 (2), pp. 133-152 (2011)

Thank you very much for giving me an opportunity to contribute to this important policy process.

Verband Deutscher Zeitschriftenverleger (VDZ – BDZV)

I. Vorbemerkung

Das Datenschutzrecht ist seit jeher für wesentliche Bereiche der Pressetätigkeit relevant. Redaktionelle Pressefreiheit ist ohne Ausnahmen vom Datenschutzrecht nicht möglich. Adressiertes Direktmarketing klassischer wie digitaler Presseabonnements ist für den Erhalt der Leserschaft unverzichtbar. Die Digitalisierung und die damit einhergehenden strukturellen Herausforderungen erfordern einen verstärkten Ausbau der digitalen Angebote der Verlage.

Die deutschen Zeitschriften- und Zeitungsverleger verfolgen daher auch die Diskussionen über die Modernisierung der Konvention 108 mit großem Interesse. Wichtig ist in diesem Zusammenhang, dass im Rahmen der Modernisierung keine Vorgaben eingeführt werden, die das auf europäischer Ebene mühsam errungene Gleichgewicht zwischen den legitimen Interessen des Einzelnen und den Kommunikationsnotwendigkeiten einer modernen Wirtschaft belasten. Hinzu kommt, dass mit der Veröffentlichung des Kommissionsvorschlags für eine EU-Datenschutzverordnung am 25.01.2012 auf europäischer Ebene gerade die Überarbeitung des EU-Rechtsrahmens begonnen hat. Den Ergebnissen der sich nun anschließenden Diskussionen auf europäischer und nationaler Ebene im Rahmen des Gesetzgebungsverfahrens sollte nicht vorgegriffen werden.

Im Zusammenhang mit der Überarbeitung des Rechtsrahmens für den Datenschutz sind für Zeitschriften- und Zeitungsverleger jedoch generell die folgenden Aspekte relevant:

- **Robuste Bereichsausnahme für die journalistische Datenverarbeitung erforderlich.** Die Anwendung der Datenschutzvorschriften auf die journalistische Datenverarbeitung 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 (siehe auch II. Ziffer 5).

- **Direktmarketing als wesentliche Voraussetzung freier und unabhängiger Presse muss weiter sachgerecht möglich bleiben.** Die freie und unabhängige Presse sowie die Medienvielfalt hängen in hohem Maße von der Möglichkeit ab, effektiv für Zeitschriften und Zeitungen zu werben. Es ist daher insbesondere unabdingbar, dass die Datenverarbeitung für zentrale Bereiche des Direktmarketings weiterhin ohne Einwilligung, aber mit Information und Widerspruchsmöglichkeit, zulässig bleibt (siehe II. Ziffern 1-4).

- **Digitale Geschäftsmodelle dürfen nicht belastet werden.** Digitale Geschäftsmodelle von der Werbung in der digitalen Presse über die Bewerbung digitaler Abonnements bis hin zum E-Commerce sind unverzichtbar. Die Überarbeitung der Datenschutzrichtlinie darf daher nicht dazu führen, die Nutzung und weitere Entwicklung solcher Geschäftsmodelle unverhältnismäßig zu beeinträchtigen oder unmöglich zu machen (siehe II. Ziffern 1 – 4).

II. Konkrete Aspekte bezogen auf den Entwurf für die Modernisierung der Konvention 108 vom 5. März 2012

1. Definition of „personal data" (Art. 2 a). Die Definition von „personal data" soll nach dem vorliegenden Entwurf unverändert bleiben. Der Explanatory Report soll jedoch unter anderem um die Aussage ergänzt werden, "'identifiable" does not only refer to the individual's civil identity but also and foremost to what allows to "individualise" one person amongst others". Dies führt letztendlich dazu, dass die Menge der als personenbezogene Daten angesehenen Informationen ein nicht mehr überschaubares Maß erreicht. Denn durch Betonung *der Möglichkeit der Individualisierung* könnten wesentlich mehr Daten als bisher als personenbezogen angesehen werden.

Diese Konsequenz wird auch nicht dadurch ausgeschlossen, dass in dem Explanatory Report eingegrenzt werden soll, „an individual is not considered "identifiable" if identification requires unreasonable time and effort for a person who would be informed of it". Nicht näher definiert wird zunächst, unter welchen Voraussetzungen von „unreasonable time and effort" ausgegangen werden kann. Hinzu kommt, dass selbst, wenn man diese Einschränkung weit interpretiert, noch immer eine erhebliche Anzahl an Informationen als „personal data" eingestuft werden könnten.

Der somit mögliche weite Anwendungsbereich und die damit einhergehenden Pflichten für die Verarbeitung der entsprechenden Informationen führen für Unternehmen zu einem nicht mehr überschaubaren Aufwand. Angesichts der möglicherweise betroffenen unterschiedlichen Kategorien von Daten, von denen viele nach geltender Rechtslage wohl nicht als personenbezogen angesehen würden, ist dieser Aufwand in vielen Fällen wohl auch mangels Schutzbedürftigkeit aus Verbraucherschutzgesichtspunkten nicht gerechtfertigt. Die zitierte Ergänzung des Explanatory Reports sollte daher wieder gestrichen werden.

2. Legitimacy of data processing and quality of data (Art. 5). In dem Entwurf für einen neuen Abs. 2 des Art. 5 ist bestimmt, „Each Party shall provide that data processing can be carried out only if a) the data subject has freely given his/her specific and informed consent, or b) it is provided for by domestic law for an overriding legitimate interest or is necessary to comply with legal obligations or contractual obligations binding the subject". Durch diese Vorgaben könnten zahlreiche der nach heutiger Rechtslage möglichen und wichtigen Datenverarbeitungsprozesse erheblich belastet, wenn nicht sogar unmöglich gemacht werden.

Dies gilt zum einen, als in dem heute maßgeblichen Art. 7 der Richtlinie 95/46/EG sechs Alternativen festgelegt sind, von denen eine erfüllt sein muss, damit die Datenverarbeitung zulässig ist. Das ist auch sachgerecht, da dadurch dem Umstand Rechnung getragen werden kann, dass es viele unterschiedliche Situationen gibt, in denen Daten legitimerweise verarbeitet werden müssen. Nach dem vorliegenden Vorschlag soll es jedoch nur noch vier Alternativen geben.

Zum anderen lässt sich nicht ausschließen, dass die Möglichkeiten der Datenverarbeitung zur Verfolgung legitimer Interessen des Verarbeitenden und Dritter ohne vorherige Einwilligung, aber mit Information und der Möglichkeit zum Widerspruch, weiter eingeschränkt werden (derzeit zulässig gemäß Art.7 f) der Richtlinie 95/46/EG). Denn festgelegt wird, dass die Zulässigkeit der entsprechenden Datenverarbeitung im nationalen Recht festgelegt werden soll. Hierbei muss man berücksichtigen, dass die Überarbeitung des EU-Rechtsrahmens für den Datenschutz gerade darauf abzielt, ein europaweit einheitliches Recht zu schaffen, und in eine Verordnung münden soll. Nach dem Entwurf der EU-Kommission werden die Bedingungen für die zulässige Datenverarbeitung daher direkt in der Verordnung festgelegt, ohne dass noch eine Umsetzung in nationales Recht erforderlich wäre. Sichergestellt werden muss daher, dass durch eine entsprechende Überarbeitung des europäischen Datenschutzrahmens diese Vorschrift nicht ausgehöhlt wird. Sachgerechterweise sollte daher diese Vorgabe um die Möglichkeit ergänzt werden, dass die entsprechende Festlegung auch in europäischem Recht erfolgen kann.

Ausgeführt wird zudem, der Explanatory Report „will explain the meaning of overriding legitimate interest (including by taking the examples of Section 7 of the Directive 96/46/EC) and that consent may be withdrawn". Richtigerweise sollten zwar die bisher in Art. 7 der Richtlinie aufgeführten Alternativen der zulässigen Datenverarbeitung weiter gelten. Sinnvollerweise sollten diese Alternativen jedoch bereits im Konventionstext selbst aufgeführt werden.

Bei etwaigen Überlegungen zur Änderung der geltenden Rechtslage muss in jedem Fall sicher gestellt werden, dass die Möglichkeiten der effektiven Leserwerbung für die Presse nicht weiter eingeschränkt werden. Es ist daher insbesondere unabdingbar, dass die Datenverarbeitung für zentrale Bereiche des Direktmarketings weiterhin ohne Einwilligung, aber mit Information und Widerspruchsmöglichkeit, möglich bleibt. Dies ist für die Presse wie für viele andere Branchen eine wichtige, und teilweise sogar die einzige, Möglichkeit, mit ihren Kunden in Kontakt zu treten oder neue Kunden zu gewinnen. Das gilt besonders für kleine und mittelständische Unternehmen, die sich keine Postwurfsendungen oder Werbung in den Massenmedien leisten können.

In Deutschland hängen bis zu 20% der Abonnementauflage vieler Zeitungen und Zeitschriften von adressiertem Direktmarketing ohne vorherige Einwilligung an Fremdadressen ab. Für das Segment lokaler und regionaler Zeitungen haben aktuelle Befragungen sogar ergeben, dass Werbebriefe an Fremdadressen bis zu 50 % der befristeten Abonnements und bis zu 20 % der neugewonnenen unbefristeten Abonnements generieren. Dieses Bild wird auch durch die Erfahrungen aus anderen europäischen Ländern bestätigt, in denen der entsprechende Anteil der Auflage sogar teilweise über 40 % ausmacht.

Bei der Fachpresse macht der Abo-Anteil regelmäßig nur einen kleinen Teil der Auflage aus. Der größte Teil der Auflage (teilweise bis ca. 90 %) wird kostenlos im sog. Frei- und Wechselversand auf der Basis spezieller Adresslisten an die jeweils relevante Zielgruppe (zum Beispiel Maschinenbauer, Bäcker oder Architekten) versandt.

3. Transparency of processing (Art. 7 bis). Die geltenden Informationspflichten wurden gegenüber dem geltenden Text erweitert. Sichergestellt werden muss jedoch, dass diese auch praktikabel sind. Dies gilt zunächst etwa für die Information über mögliche Empfänger der Daten. Hier muss es möglich sein, dass diese Information auch generalisierend erfolgen kann. Richtigerweise wird daher auch im Explanatory Report darauf hingewiesen, „the information regarding the recipients may also refer to categories of recipients". Dieser Hinweis sollte daher auch in den endgültigen Text übernommen werden.

Hinzu kommt, dass es für Unternehmen nicht rechtssicher ersichtlich ist, welche Informationen zur Verfügung gestellt werden müssen. Denn diese umfassen nach der Vorschrift auch „any other information necessary to ensure a fair data processing". In dem Explanatory Report soll zwar näher spezifiziert werden, „any information necessary to ensure a fair data processing" notably includes information on transfer to other countries". Die Einschränkung durch "notably" weist jedoch darauf hin, dass dieses Beispiel nicht abschließend gemeint ist. Die in Abs. 2 enthaltene Abwägungsklausel vermag diese Problematik ebenfalls nicht abzumildern. Denn bestimmt ist dort lediglich bestimmt, dass diese Informationen nicht zur Verfügung gestellt werden müssen, wenn „this proves to be impossible or involves disproportionate efforts". Nicht näher ausgeführt wird jedoch, wann diese Bedingung erfüllt ist.

Berücksichtigt werden muss im Zusammenhang mit der Festlegung von Informationspflichten aber auch, dass diese Informationsverpflichtungen auf allen Kommunikationswegen sinnvoll verwirklicht werden können müssen. Es muss sichergestellt werden, dass nicht durch die Festlegung von Informationspflichten traditionelle und bewährte Kommunikationswege (z. B. beim Direktmarketing für Zeitschriften und Zeitungen die Bestellkarte oder der Werbebrief) nicht mehr genutzt werden können, da sich bei diesen die Fülle an geforderten Informationen einfach nicht mehr angemessen erfüllen lässt.

Unklar ist nach der jetzigen Fassung des Entwurfes außerdem, wann die entsprechenden Informationen zur Verfügung gestellt werden müssen. Dies ist jedoch ein entscheidendes Kriterium für die Beurteilung der Praktikabilität der entsprechenden Verpflichtung. Ausgeführt ist hierzu lediglich, dass der Explanatory Report dies spezifizieren wird. Dies reicht jedoch nicht aus, um eine abschließende Beurteilung zu ermöglichen.

4. Rights of the data subject (Art. 8)

Auch die erweiterten Vorschriften zu den Rechten des Einzelnen bergen die Gefahr weiterer Belastungen für Verlage.

a) Auskunftsrecht (Art. 8 a und b). Bestimmt ist in Art. 8 a), dass der Einzelne das Recht haben soll, zu erfahren „at resonable intervals and without excessive delay or expense confirmation or whether personal data relating to him/her are being processed or not, the communication of such data in an intelligible form and all available information on the origin of the data and any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis".

Die Verpflichtung, dem Einzelnen in angemessenen Intervallen die entsprechenden Informationen zukommen zu lassen, ist nicht nur zu unbestimmt, sondern auch zu weitgehend. Zunächst wird nicht näher erläutert, was unter „reasonable intervals" zu verstehen ist. Für das einzelne Unternehmen ist damit nicht rechtssicher ersichtlich, in welchen Zeitabständen er dieser Verpflichtung nachkommen muss. Hinzu kommt, dass diese Verpflichtung unabhängig von dem gewählten Intervall zu einem erheblichen Aufwand für Unternehmen führt und in vielen Fällen auch von dem Einzelnen überhaupt nicht gewünscht sein mag. Sachgerechterweise sollte diese Auskunft daher lediglich auf Anfrage erfolgen.

In Art. 8 b) ist weiter bestimmt, dass der Einzelne auch das Recht haben soll, "to obtain knowledge of the logic involved in the data processing in the case of an automated decision". Abgesehen davon, dass diese Verpflichtung aufgrund des weiten Anwendungsbereich (siehe hierzu auch unter b)) wohl zu einem nicht mehr überschaubaren Aufwand für Unternehmen führt, dürften in zahlreichen Fällen von dieser Ausnahme auch Geschäftsgeheimnisse betroffen sein. Richtigerweise wird daher auch in dem Explanatory Report darauf hingewiesen, "the knowledge of the logic involved in the processing cannot be detrimental to legally protected secrets". Dies sollte auch in den endgültigen Text übernommen werden.

b) Decision based on automated data processing (Art. 8 e). Festgelegt wird in Art. 8 e) das Recht des Einzelnen, „not to be subject to a decision significantly affecting him/her or producing legal effects concerning him/her, based solely on the grounds of an automated processing of data without having the right to express his/her views". Aufgrund dieser weiten Formulierung birgt diese Vorschrift die Gefahr, traditionelle und bewährte Geschäftsmodelle deutlich zu belasten bzw. sogar unmöglich zu machen.

Aufgrund der generalklauselartigen Formulierung des Art. 8 e) lässt sich nicht abschließend absehen, welche Datenverarbeitungsmaßnahmen konkret darunter fallen. Nicht definiert wird insbesondere, wann eine „decision significantly affecting him/her" vorliegt. Unklar ist außerdem, unter welchen Voraussetzungen von einer „solely on the grounds of an automated processing of data" basierenden Maßnahme ausgegangen werden muss. Dies gilt insbesondere für die Fälle, in denen die entsprechende Datenverarbeitung zwar automatisiert, aber auf der Basis zuvor durch eine Person festgelegter Kriterien erfolgt.

Es lässt sich daher nicht ausschließen, dass darunter auch zahlreiche Datenverarbeitungsprozesse fallen, die für Verlage essentiell sind, wie etwa Maßnahmen im Rahmen der Kundenbindung oder sog. interessenbasierte Werbung, die als eine wichtige Werbeform im Online-Bereich zur Finanzierung digitaler Verlagsangebote relevant sein kann.

Diese Vorschriften könnten aufgrund der weiteren Formulierung sogar für Datenverarbeitungsprozesse gelten, bei denen keine Identifizierung einer bestimmten Person erfolgt, wie die Erstellung pseudonymisierter Nutzungsprofile zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

5. Exceptions and restrictions (Article 9). In Art. 9 Abs. 1 ist bestimmt, "no exception to the provisions of this Convention shall be allowed, except to the provisions of Article 5.3, 6, 7.2, 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to […] b) protect the data subject or the rights and freedom of others, notably freedom of expression and information".

Die Ausnahme geht nicht weit genug und würde die geltenden Schutzstandards für die journalistische Datenverarbeitung erheblich einschränken. 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 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.

Eine entsprechende der Ausnahmen bedeutet im Übrigen nicht, dass die entsprechenden journalistischen Aktivitäten in einem rechtfreien Raum stattfinden. Diese können vielmehr weiterhin durch das jeweilige nationale Medien-, Äußerungs- und Persönlichkeitsrecht geregelt werden.

Die Ausnahme muss daher zumindest die Artikel 4-8, 10-21 vollständig umfassen, um ein vergleichbares Schutzniveau wie bisher sicher zu stellen. Auch die Vorgabe, dass es sich bei den entsprechenden Ausnahmen um „a necessary measure" handeln muss, eröffnet einen weiten Ermessenspielraum und birgt die Gefahr weiterer Einschränkungen. Daran ändert auch der Umstand nichts, dass im Explanatory Report spezifiziert werden soll, „this provision concerns data processing carried out solely for communication information to the public, ideas or opinions of general interest, or for literary or artistic expression." Diese Einschränkung sollte daher gestrichen werden.

Ansprechpartner:

VDZ
Dr. Christoph Fiedler
Geschäftsführer Europa- und Medienpolitik
Tel.: 0049 30 72 62 98 120
c.fiedler@vdz.de

BDZV
Carolin Wehrhahn
Referentin Europapolitik
Tel.: 0032 2 551 01 94
wehrhahn@bdzv.de

Dr. Karina Lott
Referentin Europa- und Medienpolitik
Tel.: 0032 2 536 06 03
k.lott@vdz.de