COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, le 02 juin 2008 T-PD (2008) RAP 24

COMITE CONSULTATIF
DE LA CONVENTION POUR LA PROTECTION DES PERSONNES
A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL [STE 108]
(T-PD)

24e réunion
Strasbourg, 13-14 mars 2008

RAPPORT DE REUNION

Document du Secrétariat preparé par la
Direction Générale des des droits de l'Homme et des affaires juridiques

TABLE DES MATIERES

ANNEXES

I. OUVERTURE DE LA RÉUNION

1. Le comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), constitué en vertu de l'article 18 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [STE n° 108], a tenu sa 24e réunion les 14 et 15 mars 2008 au Conseil de l'Europe à Strasbourg, sous la présidence de M. João Pedro CABRAL (Portugal).

2. La liste des participants fait l'objet de l'annexe I au présent rapport.

II. ADOPTION DE L'ORDRE DU JOUR

3. L'ordre du jour, adopté par le T-PD, est reproduit à l'annexe II au présent rapport accompagné de la liste des documents intéressant chacun des points examinés.

III. COMMUNICATION DU SECRÉTARIAT

4. Le T-PD prend acte des informations communiquées par le Secrétariat concernant les faits nouveaux survenus depuis sa dernière réunion (15-16 mars 2007) au sein de l'Organisation en général et du domaine de la protection des données en particulier.

5. S'agissant des faits les plus importants concernant l'Organisation, le Secrétariat apporte les informations suivantes :

6. La Direction générale des affaires juridiques et la Direction générale des droits de l'homme constituent désormais une seule et unique structure appelée Direction générale des droits de l'homme et des affaires juridiques (DG-HL) que conduit M. Philippe Boillat. En plus de la Commission de Venise, cette nouvelle direction générale se compose des trois directions suivantes :

- La Direction des activités normatives
- La Direction de la coopération
- La Direction des monitorings

7. La Direction des activités normatives comprend deux services : le Service des réformes législatives, qui couvre les activités de protection des données, et le Service du développement des droits de l'homme.

8. Cette nouvelle structure a pour objet de favoriser, entre des activités auparavant menées par l'une ou l'autre des deux anciennes directions, une synergie dont témoignent les travaux de la Division Médias et société de l'information et ceux qui intéressent la protection des données à caractère personnel et la cybercriminalité.

9. La Convention du Conseil de l'Europe pour la prévention du terrorisme (STCE n° 196) est entrée en vigueur le 1er juin 2007, ayant obtenu les six ratifications requises. A ce jour, elle a été ratifiée par douze pays et signée par trente.

10. Le Protocole additionnel à la Convention sur les droits de l'homme et la biomédecine, relatif à la recherche biomédicale (STCE n°195) est entré en vigueur le 1er septembre 2007. A ce jour, il a été ratifié par cinq Etats et signé par seize.

11. La Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains (STCE n°197) est entrée en vigueur le 1 er février 2008, avec, à ce jour, dix-sept ratifications et vingt-et-une signatures.

12. La 28e Conférence des ministres européens de la justice s'est tenue à Lanzarote (Espagne) les 25 et 26 octobre 2007 sur le thème « Nouveaux problèmes d'accès à la justice concernant les groupes vulnérables, notamment les migrants et les demandeurs d'asile, les enfants y compris les enfants délinquants ». A cette occasion, la nouvelle convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels (STCE n°201) a été ouverte à la signature. A ce jour, l'instrument a été signé par vingt-sept Etats et entrera en vigueur lorsqu'il aura obtenu au moins cinq ratifications.

Faits nouveaux dans le domaine de la protection des données à caractère personnel

13. Andorre a signé la Convention 108 le 31 mai 2007 et l'a ratifiée le 6 mai 2008 (entrée en vigueur le 1er septembre 2008), la Moldova l'ayant ratifiée le 28 février 2008 (entrée en vigueur le 1er juin 2008). En conséquence, le nombre de ratifications de cet instrument est aujourd'hui de quarante, celui des signatures non suivies de ratification étant de trois.

14. Le Protocole additionnel à la Convention 108 concernant les autorités de contrôle et les flux transfrontières de données (STCE n°181) a fait l'objet de trois nouvelles ratifications et de trois nouvelles signatures :

- la France a ratifié le Protocole le 22 mai 2007 (entrée en vigueur le 1er septembre 2007) ;
- Andorre l'a signé le 31 mai 2007 puis ratifié le 6 mai 2008 (entrée en vigueur le 1er septembre 2008) ;
- la Suisse l'a signé le 17 octobre 2007 et ratifié le 20 décembre 2007 (entrée en vigueur le 1er avril 2008) ;
- « l'ex-République yougoslave de Macédoine » l'a signé le 4 janvier 2008 ; et
- l'Autriche l'a ratifié le 4 avril 2008 (entrée en vigueur le 1er août 2008).

15. Le Protocole additionnel à la Convention 108 compte à ce jour vingt ratifications et treize signatures non suivies de ratification.

16. Les listes complètes des ratifications et des signatures des deux instruments font l'objet des annexes III et IV.

17. A la suite de l'acceptation, par la Serbie le 15 mai 2007, des amendements à la Convention 108 autorisant les communautés européennes à adhérer à l'instrument, vingt-huit des trente-neuf Etats parties ont accepté ces amendements qui entreront en vigueur lorsque toutes les Parties auront informé le Secrétaire Général de leur décision de les approuver.

18. Enfin concernant le projet sur la protection des données dans le cadre de l'état civil en Albanie lancé il y a près d'un an par le Conseil de l'Europe et l'OSCE, il a été constaté des progrès satisfaisants dans le domaine des réformes législatives : un nouveau projet de loi sur la protection des données à caractère personnel, élaboré avec le concours d'experts du Conseil de l'Europe, vient d'être adopté. Ce texte, conforme aux principes de la Convention 108, prévoit la mise en place d'un commissaire chargé de la protection des données, élu par le parlement. Dès son élection, le Conseil de l'Europe se chargera de sa formation et de celle de son personnel et continuera de mener des activités de sensibilisation s'agissant des personnes concernées et des maîtres de fichiers dans le pays.

IV. ÉLECTION DU/DE LA PRÉSIDENT(E) DE DEUX VICE-PRÉSIDENT(E)S ET DE QUATRE MEMBRES DU BUREAU

1. Conformément à l'article 10 de son Règlement Intérieur, le T-PD élit M. Joao Pedro CABRAL (Portugal) pour un second et dernier mandat consécutif à compter du 14 mars 2008. Il élit également Mme Eva SOUHRADA-KIRCHMAYER (Autriche) comme première vice-présidente et M. Jean-Philippe WALTER (Suisse) pour un second et dernier mandat

consécutif, à compter également du 14 mars 2008. La présidence rappelle que, conformément à l'article 10 bis 2 du Règlement intérieur, le président et les deux vice-présidents font automatiquement partie du Bureau.

2. S'agissant des autres membres du Bureau, le Secrétariat a lancé un appel à candidatures avant la réunion. Six demandes ont été reçues de la part de M^me^ Hana ŠTEPÁNKOVÁ (République tchèque), M^me^ Pascale COMPAGNIE (France), M^me^ Eva SILBERMANN (Allemagne), M^me^ Kinga SZURDAY (Hongrie), M^me^ Stefania CONGIA (Italie) et M^me^ Veronika ŽUFFOVÁ-KUNČOVÁ (Slovaquie). Parmi ces postulantes et conformément à l'article 10 bis 2. de son Règlement Intérieur, le T-PD a élu M^me^ Hana ŠTEPÁNKOVÁ (République tchèque), M^me^ Pascale COMPAGNIE (France), M^me^ Eva SILBERMANN (Allemagne) et M^me^ Stefania CONGIA (Italie), membres du Bureau pour un mandat renouvelable de deux ans.

V. ÉCHANGE DE VUES AVEC LE COMMISSAIRE À LA PROTECTION DES DONNÉES DU CONSEIL DE L'EUROPE, KAREL NEUWIRT

3. Le T-PD procède à un échange de vues avec M. Karel NEUWIRT, commissaire à la protection des données du Conseil de l'Europe, qu'il a élu à sa dernière réunion en 2007.

4. Le commissaire remercie d'abord le T-PD de l'avoir élu puis déclare que le Règlement du Secrétaire Général du 17 avril 1989 instaurant un système de protection des données pour les fichiers de données à caractère personnel du Conseil de l'Europe n'est plus d'actualité et n'assure pas le même niveau de protection que des organisations internationales comme INTERPOL ou EUROJUST. En effet, son annexe, qui concerne le commissaire à la protection des données, stipule que celui-ci est un expert indépendant de l'Organisation, ce qui, de ce fait, ne lui permet pas de remplir quotidiennement sa mission de contrôle du traitement des données à caractère personnel au sein du Conseil de l'Europe et implique que l'article 5 du Règlement relatif à l'établissement d'un inventaire de tous les fichiers automatisés de données à caractère personnel détenus par l'Organisation, n'a en fait jamais été appliqué. Renforcer le rôle du commissaire lui permettrait également de sensibiliser le personnel aux bonnes pratiques dans le domaine de l'étude.

5. Le commissaire signale qu'il a fait part au Directeur des activités normatives, M. Jan KLEIJSSEN, de son intention de modifier ce règlement et que celui-ci l'a encouragé dans ce sens. Le T-PD informe le commissaire de son soutien et lui indique qu'il l'aidera en cas de besoin.

VI. MÉTHODES DE TRAVAIL DU T-PD

6. Le comité examine et approuve les modifications de son Règlement intérieur afin d'améliorer ses méthodes de travail, compte tenu de la diminution constante du nombre et de la durée de ses réunions et de celles de son Bureau. La version actuelle du Règlement Intérieur fait l'objet du document T-PD (2008) 03Rev et figure sur le site Internet « Protection des données ». Le T-PD :

- décide, compte tenu de l'utilisation des nouvelles technologies, de ne plus envoyer, comme le prévoit l'article 7.2, la lettre de convocation aussi longtemps avant la date fixée pour l'ouverture de la réunion ;
- décide également, en cas d'urgence, et comme le prévoit l'article 15, de remplacer, par une procédure de décision écrite, la procédure de délégation du pouvoir de décision au Bureau. Celle-ci constituerait en effet une meilleure garantie de la participation de l'ensemble du T-PD au processus de décision, le comité estimant que, même dans les cas urgents, il est possible de voter à l'aide de dispositifs électroniques. Il souligne toutefois que, pour utiliser la procédure écrite, il faudra prévoir suffisamment de temps, pas moins de quatre semaines dans les cas habituels et de deux dans les cas urgents.

Tous les membres devront accuser réception du projet de décision par courrier électronique et respecter strictement les délais indiqués par le Secrétariat pour voter. En conséquence, le T-PD décide d'ajouter deux paragraphes (15.4 et 15.5) à l'article 15.3 et d'ajouter aussi une définition de la « procédure écrite » à l'article 1 ;

- le comité examine ensuite l'article 10.ter concernant la procédure et la question du nombre de lectures d'un projet de texte par le T-PD. Le Secrétariat propose de supprimer la mention du nombre de lectures pour permettre plus de souplesse et accélérer le processus de décision. Certains membres y sont favorables tandis que d'autres craignent que cette suppression ait un effet contraire et permette à quelques Etats membres de retarder, voire de bloquer, le processus de décision en demandant continuellement de nouvelles lectures. Le T-PD estime que ce point devrait être réexaminé et charge le Bureau de l'approfondir et de proposer un projet de texte aux fins d'adoption par procédure écrite.

VII. DROIT FONDAMENTAL A LA PROTECTION DES DONNEES

25. Le président présente ce point de l'ordre du jour, rappelle les activités pertinentes déjà menées par le T-PD et son Bureau et souligne qu'il n'a jusqu'à ce jour pas été trouvé de consensus en la matière. Il demande ensuite aux participants s'ils souhaitent continuer à examiner la question du droit fondamental à la protection des données.

26. Les représentants du Danemark, de la France, de l'Irlande, de la Slovaquie et du Royaume Uni indiquent qu'ils n'y sont pas favorables car un tel droit n'aurait guère de valeur ajoutée, l'analyse de la jurisprudence pertinente de la Cour européenne des droits de l'homme par le Bureau ayant démontré que les questions de protection des données étaient déjà couvertes par l'article 8 de la Convention européenne des droits de l'homme.

27. La représentante de la France ajoute que le texte de la Convention 108 a prouvé sa souplesse et son adaptabilité au fil des ans. Selon elle, s'il y a problème, c'est plutôt dans l'application du protocole additionnel à la Convention, question à laquelle le T-PD devrait s'intéresser.

28. Les représentants de l'Autriche, de Chypre, de la Finlande, de la Grèce, du Portugal, de la Slovénie et de l'Espagne sont prudemment favorables à l'idée de ce droit.

29. Mais la plupart des représentants (Belgique, République tchèque, Estonie, Allemagne, Lichtenstein, Lettonie, Lituanie, Luxembourg, Pays-Bas, Roumanie et Suisse), soit ne se prononcent pas, soit n'ont pas de position officielle.

30. Le représentant des Pays-Bas demande quel est le point de vue de la Commission européenne, ce à quoi son délégué répond que celle-ci n'en a pas encore mais que si cette initiative devait se concrétiser, une coordination à l'échelon de la communauté, voire une position officielle de l'Union européenne, serait nécessaire.

31. Etant donné l'absence de consensus, le représentant de la Suisse propose de reprendre la question lors de la prochaine réunion plénière du T-PD en mars 2009. D'ici là, les Etats membres de l'Union européenne auront tous ratifié le traité de Lisbonne et les communautés européennes en auront peut-être fait autant pour la Convention européenne des droits de l'homme ce qui pourrait faire évoluer les choses. En conséquence, le T-PD est convenu de réexaminer la situation en mars 2009.

VIII PROFILAGE

32. L'équipe d'experts scientifiques, dirigée par Yves Poullet et Jean-Marc Dinant, présente l'étude de ces derniers sur l'application de la Convention 108 au mécanisme de profilage (voir annexe V). Le texte intégral de l'étude fait l'objet du document T-PD (2008) 1. Cette présentation est suivie d'une discussion qui porte essentiellement sur la conclusion du texte et sur la proposition d'élaboration d'une nouvelle recommandation pertinente.

33. Le T-PD est favorable à l'élaboration d'un projet de recommandation sur le profilage. Le Secrétariat précise que puisque le T-PD est un comité composé des représentants des Etats parties à la Convention 108, ses recommandations ne peuvent s'adresser qu'aux Etats parties. Pour qu'une recommandation approuvée par le T-PD devienne une recommandation du Comité des Ministres, il faut qu'elle soit portée à l'attention du comité directeur compétent – à l'heure actuelle le comité européen de coopération juridique (CDCJ) dont le mandat couvre la question de la protection des données à caractère personnel – qui recommandera au Comité des Ministres d'adresser la recommandation du T-PD à l'ensemble des Etats membres. Cette procédure est rendue nécessaire par la dissolution du CJPD, le Comité intergouvernemental sur la protection des données, qui élaborait des projets de recommandation aux Etats membres sous l'égide du CDCJ.

34. Le représentant de la Commission européenne souligne qu'une coordination à l'échelle des communautés sera nécessaire si le Conseil de l'Europe devait élaborer une recommandation sur le profilage.

35. Le T-PD examine brièvement le champ d'application du texte à rédiger. Le représentant de l'Autriche souhaiterait qu'il soit vaste et englobe le profilage criminel.

36. Analysant les trois étapes du profilage décrites dans l'étude susmentionnée, les participants estiment tous que le projet de recommandation devra évidemment porter sur la troisième et dernière étape du processus qui consiste à appliquer le mécanisme de profilage à des personnes identifiées ou identifiables. Certains membres se demandent toutefois s'il pourrait également porter sur les deux premières étapes, à savoir l'entreposage de données *(« data warehousing »)* et l'exploitation stratégique des données *(« data mining »).* Ils estiment en effet, comme le dit l'étude, que la Convention 108 n'est pas applicable en particulier à l'étape d'exploitation stratégique des données où ces dernières sont totalement anonymes. En revanche, la recommandation R (97) 18 concernant les statistiques est applicable aux deux premières étapes.

37. D'autres membres ainsi que les experts scientifiques souhaiteraient que le projet de recommandation porte sur toutes les trois étapes. Les experts soulignent que le glissement de l'exploitation stratégique des données (deuxième étape) au profilage individuel (troisième étape) est imperceptible et qu'il est donc difficile de n'appliquer les mesures qu'à la troisième étape. La recommandation précitée sur les statistiques, qui envisage les données anonymes à la lumière des risques qu'elles font peser sur la vie privée, est un autre argument en la matière. En effet cette recommandation précise (voir 4.1) que les statistiques ne doivent pas être utilisées pour prendre des décisions et des mesures concernant les personnes privées et qu'elles n'offrent donc pas de protection dans le cas du profilage. Si le Conseil de l'Europe a estimé utile d'adopter une recommandation concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques, il devrait le faire d'autant plus dans le cas du profilage qui fait peser des risques accrus sur la vie privée et constitue un domaine très peu réglementé.

38. Le T-PD décide donc d'examiner, au moins à titre préparatoire, le processus de profilage dans son intégralité.

39. Concernant l'étude, il est convenu de la publier sur le site Internet du Conseil de l'Europe sur la protection des données[1]. La possibilité d'organiser une consultation publique y relative est brièvement envisagée, la plupart des représentants estimant toutefois plus utile, si cette consultation devait avoir lieu, de la faire porter sur le du texte du T-PD. L'étude d'experts, qui exprime le point de vue de ses auteurs et pas nécessairement celui du Conseil de l'Europe, devra servir de base aux activités futures du comité en la matière.

IX. STATUT ET POUVOIRS DES AUTORITÉS DE CONTRÔLE DE LA PROTECTION DES DONNÉES

40. Le Bureau présente au T-PD ses activités menées l'an passé concernant le statut et les pouvoirs des autorités de contrôle de la protection des données et lui demande l'autorisation de les poursuivre en 2008 ainsi que des indications sur la marche à suivre.

41. Le représentant de la Suisse estime que les travaux du T-PD et du Bureau sur cette question devraient consister en un texte interprétatif du Protocole additionnel. L'élaboration du projet de liste de critères (document T-PD-BUR (2007) 7 rev) n'a guère avancé. Les activités futures du Bureau devraient porter exclusivement sur l'application du Protocole additionnel dans les Etats parties afin de trouver des éléments propres à compléter l'interprétation de ce texte.

42. Le représentant du Danemark estime que les activités exploratoires et explicatives du T-PD concernant le Protocole additionnel seront utiles tant qu'elles n'aboutiront pas à une série d'obligations à remplir par les autorités de contrôle.

43. Plusieurs membres mentionnent la question de l'indépendance, donnant comme exemple les difficultés d'interprétation dans le cas de plusieurs Länder allemands où l'indépendance de certaines autorités régionales de contrôle est remise en cause par la Commission européenne et la Cour européenne de justice.

44. En conclusion, le T-PD décide de charger le Bureau de poursuivre les activités sur cette question et de lui en rendre compte à sa prochaine réunion plénière.

X. QUESTIONS D'ACTUALITÉ

10.1 Protection des données dans le domaine de la coopération policière et judiciaire

45. Le T-PD procède à un bref échange d'informations concernant la situation actuelle en matière de coopération policière et judiciaire au sein de l'Union européenne.

10.2 Proposition de l'Agence mondiale antidopage aux fins d'une norme sur la protection des données

46. Le Secrétariat signale qu'à la suite des prises de contact entre le Conseil de l'Europe – par l'intermédiaire du groupe de suivi de la Convention contre le dopage (T-DO) et du T-PD – et l'Agence mondiale antidopage, cette dernière a accepté qu'un article réglementant la protection des données à caractère personnel des athlètes soit ajouté au Code mondial antidopage. Au nom du T-PD, le Secrétariat a indiqué que le comité était prêt à continuer à contribuer à la rédaction de cet article. Le T-DO et l'AMA ayant volontiers accepté cette proposition de collaboration, il sera organisé dans les semaines à venir une réunion sur le projet de norme, avec la participation de quelques experts des deux comités et de l'Agence mondiale antidopage.

47. Pour ce qui est des suggestions faites par le T-PD au T-DO et à l'AMA concernant la base de données ADAMS, le Secrétariat signale qu'il n'y a eu ni fait nouveau ni demande de suite à donner en la matière.

[1] www.coe.int/dataprotection

48. Le T-PD se félicite de la grande avancée que constitue l'accord sur l'ajout d'une norme relative à la protection des données dans le Code mondial antidopage estimant que celui-ci a une portée mondiale. Il espère que le texte à élaborer assurera une protection satisfaisante.

10.3 Adhésion d'Etats non européens à la Convention 108

49. Le T-PD procède à un échange de vues concernant les faits nouveaux et les possibilités d'adhésion d'Etats non européens à la Convention 108.

50. Le président, en sa qualité de représentant du Portugal, signale qu'à l'occasion d'une conférence sur la protection des données tenue à Lisbonne par la communauté des pays hispanophones et lusophones, l'Uruguay a fait savoir qu'il souhaitait adhérer à la convention. L'orateur rappelle également que le Cap Vert vient d'adopter une législation dans le domaine à l'étude.

51. Le représentant de la Suisse indique qu'à l'occasion de la 29e Conférence internationale des commissaires à la protection des données et de la vie privée, tenue à Montréal l'an dernier, les autorités de contrôle des pays francophones ont créé une association. Celle-ci est présidée par le commissaire québécois, les vice-présidents étant le commissaire du Burkina-Faso et lui-même, le secrétaire étant quant à lui le directeur de la Commission nationale de l'informatique et des libertés (CNIL). Cette association a pour objet de favoriser la protection des données à caractère personnel dans les pays francophones et d'aider les Etats qui le souhaitent à adopter une nouvelle législation dans ce domaine. Le Bureau de l'association estime que plusieurs pays pourraient adhérer à la Convention 108.

52. Par ailleurs, poursuit l'orateur, l'association souhaiterait obtenir le statut d'observateur auprès du T-PD et lui a demandé d'interroger le comité dans cet objectif. Ce dernier a indiqué qu'il se féliciterait de cette demande.

53. Enfin le représentant de la Suisse rappelle la déclaration finale de la Conférence des commissaires à la protection des données et de la vie privée tenue à Montreux en 2005[2], qui demandait au Conseil de l'Europe, conformément à l'article 23 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, d'inviter les Etats non membres du Conseil de l'Europe qui ont une législation de protection des données, à adhérer à la convention et à son Protocole additionnel. L'orateur estime que cette invitation arriverait à point nommé car ces adhésions permettraient de faire progresser l'instauration d'un droit universel à la protection des données très attendu et qui devient de plus en plus important dans notre monde actuel de télécommunications sans frontières. Elles contribueraient également à renforcer la visibilité du Conseil de l'Europe dans ce domaine.

54. Le T-PD décide, puis recommande, que les Etats non membres dotés d'une législation de protection des données conforme à la Convention 108, soient autorisées à adhérer à l'instrument. Il invite le Comité des Ministres à prendre acte de cette recommandation et à en tenir compte lors de l'examen des demandes d'adhésion.

XI. PRÉSENTATION DES ACTIVITÉS DE LA DIVISION MÉDIAS ET SOCIÉTÉ DE L'INFORMATION

55. Le T-PD écoute le délégué de la Division Médias et société de l'information (Direction générale des droits de l'homme et des affaires juridiques) présenter les activités de sa division (voir annexe VI) dont certaines ont un rapport avec la protection des données. Le comité se félicite de cette présentation et espère que les échanges de vues se multiplieront et que la collaboration se renforcera entre les deux entités.

[2] http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf

XII. INFORMATION SUR LA JOURNÉE 2008 DE LA PROTECTION DES DONNÉES ET SUR LES DÉVELOPPEMENTS MAJEURS INTERVENUS DANS LE DOMAINE DE LA PROTECTION DES DONNÉES DEPUIS LA 23E RÉUNION DU T-PD (15-16 MARS 2007)

56. Faute de temps, le T-PD ne peut procéder au tour de table traditionnel sur les faits nouveaux intervenus depuis la dernière réunion et les initiatives prises à l'occasion de la Journée 2008 de la protection des données. En conséquence, le Secrétariat demande aux participants de soumettre ces informations par écrit. (Celles-ci font l'objet de l'annexe VII.)

XIII. DATE DES PROCHAINES RÉUNIONS

57. Le T-PD décide de tenir sa prochaine réunion plénière les 11 et 12 mars 2009 sous réserve des crédits nécessaires au budget 2009.

58. Le Secrétariat rappelle les dates et lieux des futures réunions du Bureau : 10-11 juin et 13-14 octobre à Strasbourg et 17-18 décembre à Paris.

ANNEXE I - LISTE DES PARTICIPANTS

MEMBERS OF THE T-PD/MEMBRES DU T-PD

ALBANIE/ALBANIA

Mme Zhaneta Dhima, Expert, INSTAT, Tirana

AUSTRIA/AUTRICHE

Mrs Eva Souhrada-Kirchmayer, *[First Vice-Chair of the T-PD],* Head of the data protection division, Federal Chancellery, Vienna

BELGIUM/BELGIQUE

M. François Danieli, Attaché, Ministère de la Justice, Service Public Fédéral Justice, DG "Législation et Droits fondamentaux", Service des Droits de l'Homme, Cellule "vie privée & protection des données"

CROATIA/CROATIE

Mr.Igor Vulje, Croatian Personal Data protection Agency, Zagreb

CYPRUS/CHYPRE

Mrs Nonie Avraam, Office of the Commissioner for personal data protection, Nicosia

CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE

Ms Hana Štěpánková, Communication Department, the Office for Personal Data Protection, Prague

DENMARK/DANEMARK

Inge Birgitte Moeberg, Fuldmægtig/Head of Section, København

ESTONIA/ESTONIE

Mr Urmas KUKK, Director General, Data protection Inspectorate, Tallinn

FINLAND/FINLANDE

Ms Leena Vettenranta, Counsellor of Legislation, Ministry of Justice

FRANCE

Mme Pascale Compagnie, Magistrat, Commissaire du Gouvernement auprès de la CNIL (Commission nationale de l'informatique et des libertés), Services du Premier Ministre, Paris

GEORGIA/GEORGIE

Mrs Ana Doborjginidze, 1st Secretary, Ministry of Foreign Affairs, Tbilissi

GERMANY

Eva Inés Silbermann, legal Councel/Judge, Ministry of the Interior, Data Protection Law, Berlin

GRECE/GREECE

Mr Evangelos Papakonstantinou, Lawyer, Ministry of Justice

HUNGARY/HONGRIE

Excusé/excused

IRELAND/IRLANDE

Ms Noreen Walsh, Civil Law Reform Division, Department of Justice, Equality and Law Reform, Dublin

ITALY/ITALIE

Mme Stefania Congia, Garante per la Protezione dei Dati Personali, Rome

LATVIA/LETTONIE

Evita Dzanuskane, Head of Development Division, Data State Inspectorate of Latvia, Riga

LIECHSTENSTEIN

M. Philipp Mittelberger, Datenschutzbeauftragter, Stabsstelle für Datenschutz (Data Protection Office), Vaduz

LITHUANIA/LITUANIE

Mrs Rita Vaitkevičienė, Deputy Director, State Data Protection Inspectorate, Vilnius

LUXEMBOURG

M. Gérard Lommel, Président de la Commission Nationale pour la protection des données, Luxembourg

MALTA/MALTE

Excusé/excused

MOLDOVA

Mme Valentina Popovici, Deputy Head of Division for Development of Informational Society of the Ministry of Information Development of the Republic of Moldova, Chisinau

NETHERLANDS/PAYS-BAS

Ms Anne-Marije Fontein-Bijnsdorp, Senior International Officer, College Bescherming Persoonsgegevens (Data Protection Authority), the hague

NORWAY/NORVEGE

Per Eirik Vigmostad Olsen, Adviser, Legislation department, the Norwegian Ministry of Justice, Oslo

PORTUGAL

Mr Joao Pedro Cabral, *[Chair of the T-PD],* Legal Adviser, Ministry of Justice, Lisboa

ROMANIA/ROUMANIE

Mr George Grigore, Department of European Integration, and International Affairs - Romanian DPA, Bucharest

SERBIA/SERBIE

Mrs Danica Stojanovic, Councillor, Department for International Cooperation and European Integration, Ministry of Justice, Belgrade

SLOVAKIA/SLOVAQUIE

Ms. Veronika Žuffová–Kunčová, LL.M, Head of Foreign Relations Department, Personal Data Protection Office of the SR, Bratislava

SLOVENIA/SLOVENIE

Mr Marijan Conc, State Supervisor for personal data , Information Commissioner Office, Ljubljana

SPAIN/ESPAGNE

Mr. José Leandro Núñez García, Legal Advisor, International Section of the Spanish Data Protection Agency, Agencia Española de Protección de Datos, Madrid

SWITZERLAND/SUISSE

M. Jean-Philippe Walter, *[Second Vice-Chair of the T-PD],* Office du Préposé fédéral à la protection des données et à la transparence (PFPDT), Chancellerie fédérale, Berne

"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA" / « L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE »:

Ms Marijana Marusic, Director, Directorate for Personal Data Protection, Skopje

UNITED KINGDOM/ROYAUME-UNI

Mr Kevin Fraser, Head of EU Data Protection Policy, Ministry of Justice, London

COUNCIL OF EUROPE MEMBER STATES/ ETATS MEMBRES DU CONSEIL DE L'EUROPE

MONACO

Mme Isabelle Rouanet-Passeron, Secrétaire générale, Commission de Contrôle des Informations, Autorité de contrôle de Monaco

TURKEY/TURQUIE

Bilal Çalışkan, Deputy General Director, Ministry of Justice, Ankara

COMMISSAIRE A LA PROTECTION DES DONNEES DU CONSEIL DE L'EUROPE COUNCIL OF EUROPE DATA PROTECTION COMMISSIONER

M. Karel Neuwirt, Czech Republic

EXPERTS SCIENTIFIQUES/SCIENTIFIC EXPERTS

Professeur Yves Poullet, Directeur du CRID (Centre de Recherches Informatique et Droit), Faculté de Droit, Namur, Belgique

Jean-Marc Dinant, Informaticien expert auprès de la Commission Belge de la protection de la vie privée, Maître de conférence à l'Université de Namur, Namur, Belgique

COMMISSION OF THE EUROPEAN COMMUNITIES/ COMMISSION DES COMMUNAUTÉS EUROPÉENNES

M. Alain Brun, Chef de l'Unité de protection des données à la Commission Européenne, Commission européenne, Direction générale Justice, Liberté, Sécurité, Bruxelles

OBSERVERS/OBSERVATEURS

INTERNATIONAL CHAMBER OF COMMERCE (ICC) / CHAMBRE DE COMMERCE INTERNATIONALE (CCI)

Excusé/excused

SECRETARIAT

DIRECTORATE GENERAL OF HUMAN RIGHTS AND LEGAL AFFAIRS /
DIRECTION GENERALE DES DROITS DE L'HOMME ET DES AFFAIRES JURIDIQUES

Directorate of Standard-Setting / Direction des activités normatives

Mr Jan Kleijssen, Director/Directeur

Law reform / réformes législatives

- **Public and Private Law Unit/Unité du droit public et privé**

Mrs Regina Jendottìr, Head of Public and Private Law Unit/Chef de l'Unité du droit public et privé

Data Protection/protection des données

Mme Sophie Meudal-Leenders, *Secretary of the T-PD-BUREAU/Secrétaire du T-PD-BUREAU*

Mme Pelin Ataman, Project Manager Project on Data protection within the framework of the civil registry system of Albania

Mme Frédérique Bonifaix, Secretariat, Data Protection

- **Human Rights Development Department / Service du dévelopement des droits de l'Homme**
  Media and Information Society Division / Division des médias et de la société de l'information

Mr Malinowski Jan, Head of Division

Mr Lee Hibbard, Administrator

INTERPRETERS/INTERPRETES

Mme Marie-Christine Farcot
M. Nicolas Guittonneau
Mme Julia Tanner

ANNEXE II - ORDRE DU JOUR

1. OUVERTURE DE LA REUNION

2. ADOPTION DE L'ORDRE DU JOUR

3. COMMUNICATION DU SECRETARIAT

- T-PD(2007) RAP 23 — Rapport de la 22ème réunion du Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) [STE 108] (15-16 mars 2007)
- T-PD-BUR(2006) RAP 12 — Rapport de la 12ème réunion du Bureau du Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD-BUR) [ETS No. 108]) – (5-7 septembre 2007)
- T-PD-BUR(2006) RAP 13 — Rapport de la 13ème réunion du T-PD-BUR (5-7 décembre 2007)

4. ELECTION DE/DE LA PRESIDENT(E), DE DEUX VICE- PRESIDENT(E)S, ET DE CINQ MEMBRES DU BUREAU

5. ECHANGE DE VUES AVEC LE COMMISSAIRE A LA PROTECTION DES DONNEES DU CONSEIL DE L'EUROPE, KAREL NEUWIRT

6. METHODES DE TRAVAIL DU T-PD

Action requise: le T-PD sera invité à débattre de ses méthodes de travail et à examiner une proposition de modification de son règlement intérieur aux fins de l'introduction d'une procédure écrite d'adoption de documents.

- T-PD(2008) 03 — Proposition de modification du règlement intérieur du T-PD

7. DROIT FONDAMENTAL À LA PROTECTION DES DONNEES

Action requise: le T-PD sera invité à examiner une proposition d'insertion d'un droit fondamental à la protection des données dans la Convention européenne des droits de l'Homme.

- T-PD-BUR(2006)RAP 13 — Annexe III du rapport de la 13ème réunion du T-PD-BUR (5-7 décembre 2007)
- T-PD(2008)Inf 01 — La protection des données en tant que droit fondamental par le Professeur Stefano Rodotà

8. PROFILAGE

Action requise: le T-PD entendra la présentation par le Professeur Yves Poullet et Jean-Marc Dinant de leur étude sur l'application de la Convention 108 au processus de profilage et décidera du suivi approprié.

- T-PD(2008) 01 — Version finale de l'étude de sur l'application de la Convention 108 aux mécanismes du profilage
- T-PD-BUR(2007) 05 — Eléments sur le profilage : Contributions des membres du Bureau

9. STATUT AND POUVOIRS DES AUTORITES DE CONTROLE DE LA PROTECTION DES DONNEES

Action requise: le T-PD sera informé du travail effectué par le Bureau sur ce sujet en 2007 et sera invité à confirmer les orientations suivies.

• T-PD-BUR(2007) 07Rev Restreint	Projet de liste de critères liés à la définition des autorités de contrôle de la protection des données
• T-PD-BUR13(2007)Inf 01 English only - Restreint	Document "Self Evaluation Tool for New Member States" from the Office of the Data Protection Ombudsman / Finland
• T-PD-BUR12(2007)Inf 02 English only - Restreint	Summary of the results of the questionnaire referring to the year 2006 - Questionnaire for the Spring Conference of European Data Protection Authorities, Larnaka, 10-11 May 2007
• T-PD-BUR12(2007)Inf 03 English only - Restreint	Questionnaire On Requests for Information put to a controller, Complaints, Audits and Sanctions, and on their Implementation By the Task force on Enforcement of the Working Party 29
• T-PD(2008)Inf 02	Caractéristiques principales des Autorités de contrôle de protection des données et procédures pour leur mise en place par Giovanni Buttarelli (Conférence de Madrid 2002)

10. QUESTIONS D'ACTUALITE

Action requise: le T-PD aura un échange de vues sur les questions d'actualité afin de décider le cas échéant d'un suivi approprié.

10.1 Protection des données dans le domaine de la coopération policière et judiciaire

10.2 Proposition de l'Agence mondiale anti-dopage d'un standard sur la protection des données

- T-PD(2008)Inf 03

Adhésion d'Etats non Européens à la Convention 108

11. PRESENTATION PAR LA DIVISION DES MEDIA ET DE LA SOCIETE DE L'INFORMATION DE LEURS ACTIVITES

12. INFORMATION SUR LA JOURNEE 2008 DE LA PROTECTION DES DONNEES ET SUR LES DEVELOPPEMENTS MAJEURS INTERVENUS DANS LE DOMAINE DE LA PROTECTION DES DONNEES DEPUIS LA 23E REUNION DU T-PD (15-16 MARS 2007)

*Action requise: étant donné les contraintes de temps, il ne sera pas possible de procéder à un échange de vues sur ces sujets. Les délégations sont donc invitées à faire parvenir par écrit leurs contributions au secrétariat avant le **7 mars 2008**.*

• T-PD-BUR13(2007) Inf 02	Compilation des formulaires de participation sur la journée de la protection des données 2008
• T-PD (2008) 02 mos	Communications sur les développements récents intervenus dans le domaine de la protection des données au niveau national

13. DATE DE LA 25E REUNION DU T-PD : 12-13 MARS 2009

ANNEXE III – STCE no. 108 Etat des signatures et ratifications

Ouverture à la signature
Lieu : Strasbourg
Date : 28/1/1981

Entrée en vigueur
Conditions : 5 Ratifications.
Date : 1/10/1985

Situation au 3/6/2008

Etats membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	9/6/2004	14/2/2005	1/6/2005	44		X	X			
Allemagne	28/1/1981	19/6/1985	1/10/1985	44		X	X	X		
Andorre	31/5/2007	6/5/2008	1/9/2008			X	X			
Arménie										
Autriche	28/1/1981	30/3/1988	1/7/1988	44		X	X			
Azerbaïdjan										
Belgique	7/5/1982	28/5/1993	1/9/1993	44		X	X			
Bosnie-Herzégovine	2/3/2004	31/3/2006	1/7/2006							
Bulgarie	2/6/1998	18/9/2002	1/1/2003							
Chypre	25/7/1986	21/2/2002	1/6/2002	44			X			
Croatie	5/6/2003	21/6/2005	1/10/2005	44		X	X			
Danemark	28/1/1981	23/10/1989	1/2/1990	44			X	X		
Espagne	28/1/1982	31/1/1984	1/10/1985			X	X			
Estonie	24/1/2000	14/11/2001	1/3/2002	44		X	X			
Finlande	10/4/1991	2/12/1991	1/4/1992	44			X			
France	28/1/1981	24/3/1983	1/10/1985	44		X	X			
Géorgie	21/11/2001	14/12/2005	1/4/2006							
Grèce	17/2/1983	11/8/1995	1/12/1995	44						
Hongrie	13/5/1993	8/10/1997	1/2/1998	44		X	X			
Irlande	18/12/1986	25/4/1990	1/8/1990	44		X	X			
Islande	27/9/1982	25/3/1991	1/7/1991	44			X			
Italie	2/2/1983	29/3/1997	1/7/1997			X	X			
Lettonie	31/10/2000	30/5/2001	1/9/2001	44		X	X			
l'ex-République yougoslave de Macédoine	24/3/2006	24/3/2006	1/7/2006			X	X			
Liechtenstein	2/3/2004	11/5/2004	1/9/2004	44		X	X			
Lituanie	11/2/2000	1/6/2001	1/10/2001	44			X			
Luxembourg	28/1/1981	10/2/1988	1/6/1988	44		X	X			
Malte	15/1/2003	28/2/2003	1/6/2003							
Moldova	4/5/1998	28/2/2008	1/6/2008			X	X			
Monaco										
Monténégro	6/9/2005	6/9/2005	6/6/2006	56						
Norvège	13/3/1981	20/2/1984	1/10/1985	44		X	X	X		
Pays-Bas	21/1/1988	24/8/1993	1/12/1993	44		X	X	X		
Pologne	21/4/1999	23/5/2002	1/9/2002	44						
Portugal	14/5/1981	2/9/1993	1/1/1994	44			X			

République tchèque	8/9/2000	9/7/2001	1/11/2001	44			X			
Roumanie	18/3/1997	27/2/2002	1/6/2002			X	X			
Royaume-Uni	14/5/1981	26/8/1987	1/12/1987	44		X	X	X		
Russie	7/11/2001									
Saint-Marin										
Serbie	6/9/2005	6/9/2005	1/1/2006	44		X	X			
Slovaquie	14/4/2000	13/9/2000	1/1/2001	44			X			
Slovénie	23/11/1993	27/5/1994	1/9/1994				X			
Suède	28/1/1981	29/9/1982	1/10/1985	44			X			
Suisse	2/10/1997	2/10/1997	1/2/1998	44		X	X			
Turquie	28/1/1981									
Ukraine	29/8/2005									

Etats non membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.

Nombre total de signatures non suivies de ratifications :	3
Nombre total de ratifications/adhésions :	40

Renvois :(44) Partie ayant accepté les amendements du 15 juin 1999 permettant l'adhésion des Communautés européennes à cette Convention.
(56) Dates de signature et de ratification par l'union d'état de Serbie-Monténégro.
a.: Adhésion - s.: Signature sans réserve de ratification - su.: Succession - r.: signature "ad referendum".
R.: Réserves - D.: Déclarations - A.: Autorités - T.: Application territoriale - C.: Communication - O.: Objection.

Source : Bureau des Traités sur http://conventions.coe.int

ANNEXE IV – STCE no. 181 Etat des signatures et ratifications

Ouverture à la signature
Lieu : Strasbourg
Date : 8/11/2001

Entrée en vigueur
Conditions : 5 Ratifications.
Date : 1/7/2004

Situation au 3/6/2008

Etats membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	9/6/2004	14/2/2005	1/6/2005							
Allemagne	8/11/2001	12/3/2003	1/7/2004			X				
Andorre	31/5/2007	6/5/2008	1/9/2008				X			
Arménie										
Autriche	8/11/2001	4/4/2008	1/8/2008							
Azerbaïdjan										
Belgique	30/4/2002									
Bosnie-Herzégovine	2/3/2004	31/3/2006	1/7/2006							
Bulgarie										
Chypre	3/10/2002	17/3/2004	1/7/2004							
Croatie	5/6/2003	21/6/2005	1/10/2005							
Danemark	8/11/2001									
Espagne										
Estonie										
Finlande	8/11/2001									
France	8/11/2001	22/5/2007	1/9/2007							
Géorgie										
Grèce	8/11/2001									
Hongrie	30/3/2004	4/5/2005	1/9/2005							
Irlande	8/11/2001									
Islande	8/11/2001									
Italie	8/11/2001									
Lettonie	22/5/2007	21/11/2007	1/3/2008							
l'ex-République yougoslave de Macédoine	4/1/2008									
Liechtenstein										
Lituanie	8/11/2001	2/3/2004	1/7/2004							
Luxembourg	24/2/2004	23/1/2007	1/5/2007							
Malte										
Moldova										
Monaco										
Monténégro										
Norvège	8/11/2001									
Pays-Bas	12/5/2003	8/9/2004	1/1/2005					X		
Pologne	21/11/2002	12/7/2005	1/11/2005							
Portugal	8/11/2001	11/1/2007	1/5/2007							
République tchèque	10/4/2002	24/9/2003	1/7/2004							

Royaume-Uni	8/11/2001							X		
Russie	13/3/2006									
Saint-Marin										
Serbie										
Slovaquie	8/11/2001	24/7/2002	1/7/2004							
Slovénie										
Suède	8/11/2001	8/11/2001	1/7/2004							
Suisse	17/10/2002	20/12/2007	1/4/2008							
Turquie	8/11/2001									
Ukraine	29/8/2005									

Etats non membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.

Organisations internationales

Organisations	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.

Nombre total de signatures non suivies de ratifications :	13
Nombre total de ratifications/adhésions :	20

Renvois :a.: Adhésion - s.: Signature sans réserve de ratification - su.: Succession - r.: signature "ad referendum".
R.: Réserves - D.: Déclarations - A.: Autorités - T.: Application territoriale - C.: Communication - O.: Objection.

ANNEXE V

The application of the Convention 108 to profiling

By Yves Poullet & Jean-Marc DINANT
With the collaboration of Antoinette Rouvroy & Christophe Lazaro

Council of Europe,
Strasbourg, 13th March 2008

Overview of the presentation

- What is profiling ?
  - ***The profiling process***
  - ***Statistical purpose vs profiling purpose***
- To what extent profiling activities are covered by Convention 108?
  - ***Scope of application :***
    - From the questionning
      « is the profiling a personal data processing ? »
      …towards an holistic data processing approach
  - ***Teological approach :***
- Consequences and avenues of enquiry

Profiling is a process with 3 steps

1. DATA WAREHOUSING
   - Collect and store anonymous or pseudonymous « slices of life ». (biographical data).
2. DATA MINING
   - Create correlations between individuals characteristics recorded to deduce RULES.
3. PROFILING OF INDIVIDUALS
   - Apply RULES to identified or identifiable individuals in order to infer characteristics.

3

Step 1 and personal data

- During data warehousing
  - Convention 108 applicable if data linked or linkable to an identified individual
    - ***What does it mean ? Technically, an individual is identified among a population if he can be distinguished from the others (Pfitzmann) => in practice if his/her properties are unique within a dataset.***
    - ***Question : Is a traceability marker (pointer) a personal data***
    - ***Answer : Yes as long as this marker uniquely identify an individual within a dataset***
  - Convention 108 non applicable if data fully anonymous
    - ***i.e. at least two different individuals share the same data***
    - ***Convention does not apply to anonymous data***
    - ***Is the anonymisation a personal data processing ?***
  - Consequences of the non application of Convention 108

4

Step 2 and personal data

- During data mining
  - Assuming that the data are fully anonymous and that the granularity would sufficient to avoid biographic identification
  - The convention 108 does not apply
  - Consequences of the non application of Convention 108

Step 3 and personal data ?

- During individual profiling
  - Convention 108 is in principle and generally applicable if the profiling is an activity which consist of
    - ***Collecting personal data related to an individual***
    - ***Using those personal data as an input to a profiling model***
    - ***Using new inferred data as new data related to an identified individual***
  - Questions :
    - ***Which kind of information would be granted to the data subject ?***
    - ***May the data subject object against the profiling?***
    - ***What kind of access may be exercised ?***
    - ***And so many issues (to be continued…)***

Legal consequences of this three steps approach

1. Towards a functional approach of anonymous data
   - See ISO 15408 and Pfitzmann criteria : « anonymity of a subject means that the subject is not identifiable (i.e not uniquely characterized) within a set of subjects, the anonymity set. »
   - Whatsoever can be the set…
2. The convention 108 will not apply to step 1 and 2
   - Except if we do consider the anonymizing process as a personal data processing
3. The right to data protection does not exhaust the right to privacy
   - Art 8 CEDH remain applicable
   - Other legal rules may apply
   - Other security requirements include protection of « computer data »

The profiling process

Why to regulate profiling?

- **To provide an information symmetry among actors**
  - **Need of a paradigm shift**
    - **Data -> intelligence**
    - **Profiling induce an intelligence asymmetry**
    - **Fair trade implies symmetric information**
- **Human dignity means not to be submitted to pure statistical decisions instead of human reasoning (cfr art 15 of EU directive 95/46)**
- **Only reasonable decisions may be taken towards a human (otherwise Kafka will succeed to Orwell)**
- **Faced to an automated decision based on profiling the individual must have the right to submit his case to a human to get a reasoned and motivated human decision**
- **Notion of weapons equality between actors (data subject and data controller)**
- **There is a strong risk of individual discrimination inhibiting or raising the price of the individual access to goods and service.**

9

Why to regulate profiling ?

- **A processing with profiling purposes is more privacy killing than a processing with a statistical purpose**
  - *Processing with statistical purposes are strongly regulated by R97(18)*
    - **« statistical purposes refers to operations of collecting and processing data ...which exclude any use of the information colected for decisions or measures related to a particular person »**
    - **« When personal data have been collected and processed for statistical purposes, they might be in no case used in order to take decisions or measures towards data subjects. It concerns notably administrative, judicial, financial,... decisions...They might not be used tp complete or amend data files used for non statistical purposes(recital p.13, 68) »**
  - *A fortiori must those processing be regulated or even be forbidden as far as they involve individual decisions*

Our final conclusion : towards a new specific recommandation ?

- Vs the first step
  - What about the obligation to inform the data subject ?
  - Does the data subject benefit of a right to object ?
  - What about sensitive data ?
  - Which kind of requirements as regard the anonymisation ?
- Vs the second step
  - What does mean legitimate and specified purposes ?
  - Difficulties to determine the proportionality of data
  - What about the obligation to check the correctness of statistical inferences ?
  - Obligation to keep traces of the statistical inferences
- Vs the third step
  - Right of the data subject not to be profiled
  - Obligation to inform automatically about the use and the error rate of statiscal inferences
  - Necessity of a balance of interest
  - Strict liability of the data controller using profiling

ANNEXE VI - PRÉSENTATION PAR LA DIVISION DES MEDIA ET DE LA SOCIÉTÉ DE L'INFORMATION

Media and Information Society Division

www.coe.int/media

Steering Committee on Media and New Communication Services (CDMC)

Group of Specialists on Human Rights in the Information Society (MC-S-IS)

From Mass Media

…to Media and New Communication Services

- Setting standards with member states and observer non-state actors
- Developing tools…games, literacy, resources
- Working with key Internet non-state actors
- CoE in European and International forums

Setting Standards

...through multistakeholder cooperation

(Feb 2008) CM Declaration on **protecting the dignity, security and privacy of children on the Internet** – *concerned by profiling of info and retention of personal data concerning children for commercial purposes, declares that, other than in the context of law enforcement, should be no lasting or permanently accessible record of the content created by children which challenges their dignity,, security and privacy or otherwise renders them vulnerable now or at a later stage in their lives…*

4 CM Recommendations on:
(Mar 2008) measures to promote respect for freedom of expression and information with regard to Internet filters – *respecting private life when using and applying filters*

(Nov 2007) measures to promote the public service value of the Internet (Nov 2007) – *IGF concern about security issues and the governance of the Internet…protecting users with respect to international data transfers, etc*

(Sep 2007) promoting freedom of expression and information in the new information and communications environment – *transparency and provision of information, guidance and assistance to EMPOWER individual users, esp in situations of monitoring (Copland), determining level of personal anonymity, profiling, UGC, etc*

(Sep 2006) empowering children in the new information and communications environment – *ensuring that children have the MEDIA LITERACY skills to create, produce and distribute content in a manner which respects rights and freedoms, rights of others,* ***including respect or private life****…*

Setting Standards

...work in progress

- Human dignity
- Media literacy
- Harmful content
- Copyright

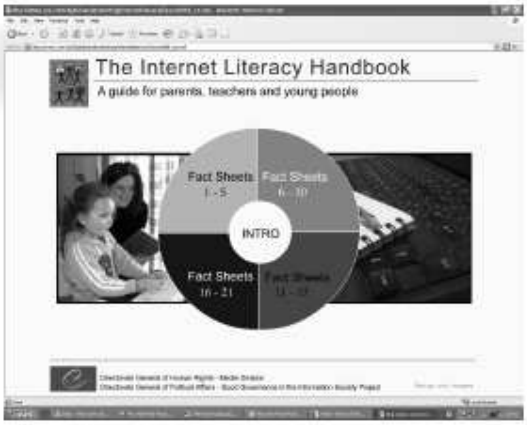
...1st Council of Europe Conference of Ministers of or responsible for Media and New Communication Services (Reykjavik, May 2009)

Developing Tools
...www.wildwebwoods.org

- Online CoE game for children helping them to learn about their rights and freedoms on Internet…collecting…privacy coins
- 14 languages +
- Over 50,000 hits (17500 users)

Developing Tools
…Handbook on Internet Literacy

- Teachers and parents
- Pragmatic classroom approach: internet privacy / why talk? / ethics / best practices / cookies
- 9 languages
- 3rd ed in 2008
- **www.coe.int/media**



Working with non-state Internet Actors

…raising awareness, encouraging responsibility

Developing human rights guidelines for key actors

- ISPs
- Social Networking Sites
- Games Providers
- Search engines

…dialogue, cooperation, ownership and visibility

CoE Organised Forums

…facilitating Pan-European dialogue

- Internet with a human face – a common responsibility (Warsaw, Mar 2004)
- Rights and responsibilities of key actors in the information society (Strasbourg, Sep 2005)
- Empowering children and young people in the new information and communications environment (Yerevan, Oct 2006)
- Ethics and human rights in the information together with UNESCO (Strasbourg, Sep 2007) (Google, CNIL etc..)

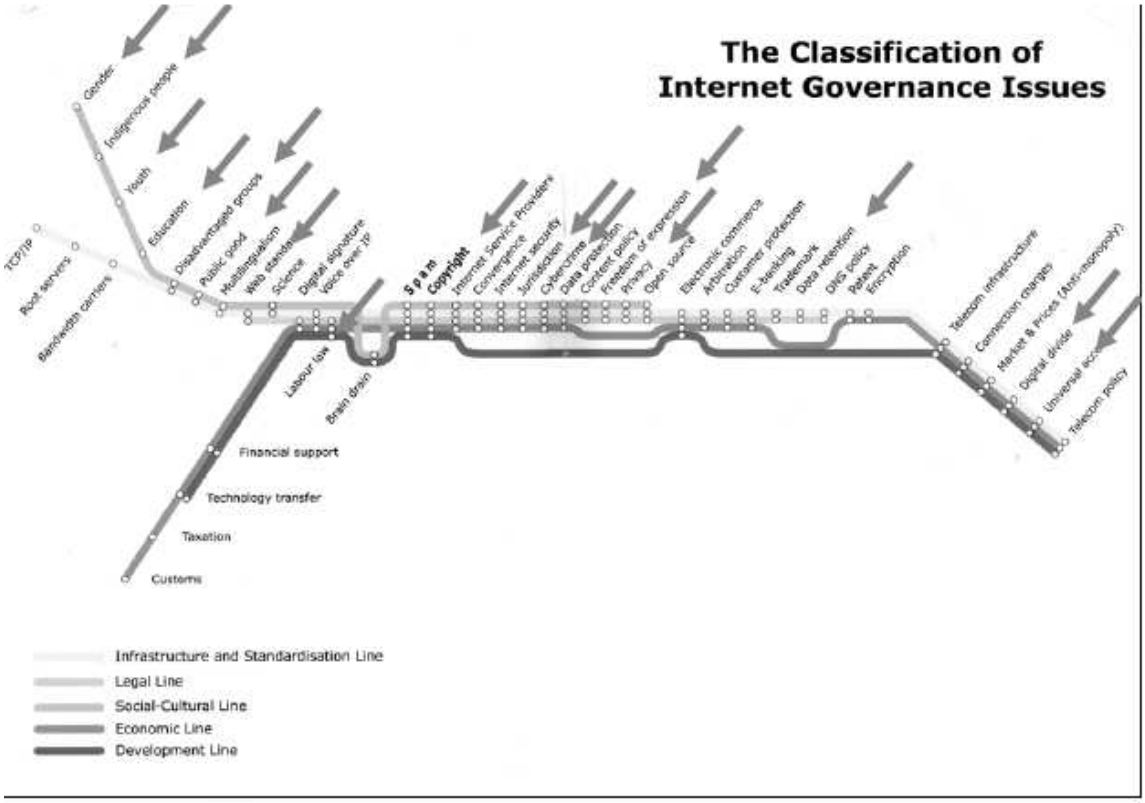
CoE in International Forums

…promoting European values and standards at the global level

UN World Summit on the Information Society (WSIS)…Geneva (2003) and Tunis (2005)

Internet Governance Forum (IGF) 2006 to 2010:

Athens, Greece, 2006 ✓
Rio de Janeiro, Brazil, 2007✓
Hyderabad, India, 2008
Cairo, Egypt, 2009
Lithuania or Azerbaijan, 2010



Global positioning systems for human rights

…in IGF-Rio (Nov 2007)

3 Main sessions (opening ceremony / openness / security)

4 CoE led/jointly organised workshops (freedom of expression / democracy / cybercrime / human rights)

2 CoE open forums (children / public service value)

4 workshops + 2 open forum organised by others in which CoE plays a key role (cybersecurity / sexual exploitation / human rights / media)

9 workshops organised by others in which CoE sits in (child pornography / child protection / privacy / security / freedom of expression : bill of rights / ICANN / UNESCO)

Statistics

Statistics WSIS (Tunis) 2005

174 states
92 IGOs
606 NGOs and civil society entities
226 business sector entities
642 media entities

IGF 2007

Approx 2000 participants

Conclusions

…and next steps

1. Right to freedom of expression and information is **intimately even inextricably linked** with the right to private and family life on the Internet;

2. CoE work on human rights in the information society is **transversal** and cannot be developed in isolation (e.g. ISPs);

3. Protecting the **privacy of children on the Internet** is a priority, especially regarding the content they generate on the Internet (sociological challenge of ceding privacy for expression and social connection)…CM Declaration on 'electronic footprint'

4. **Minimum level of public services and spaces on the Internet** which respect right to private life and data protection standards….[IGF…Right to benefit from the Information Society?]

5. 108 Convention and CoE intergovernmental work in the field of private life and data protection are **opportunities to drive forward a GPS for human rights on the Internet**

ANNEXE VII – COMMUNICATIONS SUR LES DÉVELOPPEMENTS RÉCENTS INTERVENUS DANS LE DOMAINE DE LA PROTECTION DES DONNÉES AU NIVEAU NATIONAL / INFORMATION ON RECENT DEVELOPMENTS AT NATIONAL LEVEL IN THE DATA PROTECTION FIELD

*****

ESTONIA

Passing the amendments of the Personal Data Protection Act (hereinafter PDPA), and Public Information Act (hereinafter PIA), and their partial entering into force may be considered as the most important development of the current period.

Change in division of personal data and expanding the definition of sensitive personal data by biometric data could be considered as the most important outlets of the PDPA, which was passed on February 15, 2007 and which will completely enter into force in 2008. Also the increase of protection of personal data processing, i.e. changes in regulations about processing of personal data that is given for legal public use, regulations of processing personal data for the need of research or state statistics and establishing an institution of an official responsible for personal data protection.

Since January 01, 2008, the category of private personal data does no longer exist. Personal data are divided into sensitive personal data and personal data. With vitiation of private personal data category, the mentioned duty of notifying of processing data will be also invalidated. Also, biometric data, uppermost fingerprint images, palm print and iris images, are being handled as sensitive personal data and data relating to genetic information has been replaced by the term “genetic data“.

One change the law prescribes is that a person has a right to demand the termination of disclosure and any other usage of personal data, which has been lawfully designated for public use. Therefore, a person will retain control over further usage of this data after its disclosure, which the previous wording didn’t allow.

Since January 01, 2008, the PDPA regulates collection of personal data for solvency assessment. While according to the norms valid up to this point, the time limit for collection of such data was not specifically provided, then starting from January 01, 2008, the data about personal payment default can be processed and communicated to third persons only within three years from the violation of obligations. Hence, the data in Credit Register cannot be older than three years. Older data shall be removed. Basically, the goal of this amendment is to ensure that each processor made certain the basis for processing the data and ensured that contracts, agreements and other documents were not contrary to the requirements of the law. The requirements for consent of data subject changed as well.

In the future, a person can prohibit the processing of such data, of which the legal basis for its disclosure and processing cannot be verified.

A person cannot prohibit further processing only in a case when the original disclosure took place on journalistic purposes (there are new relevant provisions in the law) or on the basis of law (for example, databases accessible to the state public).

*****

FINLAND/FINLANDE

1. Data protection legislation

Credit Information Act
The new Credit Information Act entered into force on 1 November 2007. The Act brings together provisions on credit information about consumers, companies, and relevant company personnel.

The Act includes provisions on data to be stored in credit reference records, and the period for storage of said data. The new Act defines more closely the purposes for which credit information on consumers may be disclosed and used.

Under the new Act, the Data Protection Ombudsman also oversees the processing of credit information on companies. The providers of credit information are expected to be trustworthy and to follow good credit information practice. As currently, information on the disruption of payment confirmed by authorities and notified by the debtors, as well as the credit ratings of individuals and companies can be stored in the credit reference records.

Information on any default on payment is stored in the credit reference records for a predetermined period of time. These storage times are made more precise and in some cases shortened in the new Act. While payment of debt may shorten the storage period on the one hand, the storage period can be extended, on the other hand, if the individual or company in the register is again guilty of default on payment.

The new Act will also allow companies to check their credit information and to correct any errors. Previously, such rights were only granted to natural persons. The providers of credit information must also give credit information to consumers for a reasonable compensation. The aim is that consumers can better ascertain the reliability of their contracting party.

Act on Electronic Processing of Social Welfare and Health Care Patient Data
The Act entered into force on 1 July 2007. A nationwide electronic patient database is being created in Finland, with the whole of the health care sector as users. The database is being implemented by the Social Insurance Institution of Finland, and will be gradually brought into operation from 2008 until 2011.

The database comprises storage, archiving, and transfer services of patient documents and prescriptions. The reform aims to improve the co-operation between various parties in the field of social welfare and health care and to enable the electronic transfer of data from one unit to another if the patient gives his/her consent.

The main goal is to promote security in the processing of social welfare and health care patient data and the production of health care services in a manner that is both safe for patients and effective. In addition, the new act also allows patients access to their own data and log data pertaining to its use by, for example, viewing them on-line.

All public heath care providers are required to start using the data system services. Private health care providers are obliged to join the system if the long-term retention of their patient data is conducted electronically.

Electronic Prescriptions Act
The new Electronic Prescriptions Act entered into force on 1 April 2007. The new legislation determines the requirements set for an electronic prescription system and its implementation. According to the Act, prescriptions can be drawn up electronically and transferred via data networks to the national prescription centre, which provides the information needed by the pharmacist to fill the prescription.

Physicians must tell their patients about the use of electronic prescriptions and give them written instructions on the medicine and its use. The patient has the right to refuse the electronic prescription, in which case he/she will be provided with a traditional written prescription. Because all the electronic prescriptions are stored in the prescription centre, the patients can, at any time, check the validity of their prescriptions and the amount of undelivered medicine without them having to hold on to the original prescriptions. The prescription centre and prescription archives will be maintained by the Social Insurance Institution of Finland. Prescriptions will be kept in the prescription centre for 30 months, after which they are to be transferred to the prescription archive.

If all the prescriptions of a patient have been drawn up electronically, a physician, dentist, pharmacist or qualified chemist can check the overall medication received by the patient and potential drug interactions on the basis of data provided in the prescription centre (and with the

patient's consent). Patients also have the right to receive information on who has processed or looked at data pertaining to them in the prescription centre or prescription archive.

2. The action of the Data Protection Ombudsman

2.1. The 2008 Data Protection Day in Finland

The main activity this year was to establish a permanent Public-Private -forum to promote data protection. The Data Protection Ombudsman invited several big It-companies (Microsoft, IBM, Fujitsu and some biggets local ones), representatives of universities, funding authorities etc. for this kick off -meeting where there was adopted his proposal for establishing this group. This activity therefore that the Data Protection Ombudsman find it most important and effective way to enlarge the data protection knowledgement among these key role players in information society.

The Data Protection Ombudsman has also been co-organisator in an nationwide data security day event (actually serie of events), which taked place on 12th february. This year, once again, the target groups were students in comprehensive school and ordinary consumers.

2.2. Major case law

The Court of Justice of the European Communities processes the publication of data on earned income

A Finnish company annually published the earned income of over one million Finns and passed the data on to another company for the purposes of an SMS service. This information was then passed on to the public for a fee as a commercial SMS service.

The Data Protection Ombudsman asked the competent Data Protection Board to forbid the publication of this information on earned income. The Data Protection Board has the jurisdiction to prohibit illegal processing of personal data. Contrary to the view of the Data Protection Ombudsman, the Data Protection Board, and the administrative court processing the matter after the Board, accepted the interpretation that this was a case of processing personal data for a journalistic purpose, to which the Personal Data Act is not normally applied. The processing of the matter is ongoing at the Supreme Administrative Court. On 8 February 2007, the Supreme Administrative Court requested a preliminary ruling from the Court of Justice of the European Communities, which has arranged a hearing on the matter on 12 February 2008. The Supreme Administrative Court will base its decision on the preliminary ruling.

The Supreme Administrative Court orders a bank to implement the right of full access

In February 2007, the Supreme Administrative Court agreed with the interpretation of Finnish law by the Data Protection Ombudsman in which the right of access extends to data on a client's own loan transactions and the interest rates used for them.

The bank had argued that transaction statements and interest rate data are not part of the client data files, since the microfilms containing this data are stored apart from the client data file. However, according to the Data Protection Ombudsman, this view is erroneous, because the extent of the personal data file is determined by its use. According to the Personal Data Act, data processed in order to attend to the same task belong to the same personal data file (logical data file), even though various parts of the data file (sub-registers) are stored separately. Because the purpose of using the interest data was, like other data on X, the management of a client relationship, all the data were part of the same data file. Whether they were technically stored together or apart was deemed irrelevant.

The Data Protection Ombudsman has ordered the bank to provide the client with the right of access without charge to all personal data pertaining to the client stored in the bank's personal data file. The order also pertains to loan transaction statements with the respective interest rates. In addition, the Supreme Administrative Court decided that the client had the right to check the loan transaction data pertaining to his/her own payments.

Authentication of the client in quick loan companies

The demand for quick loans requested via mobile phone or over the Internet has dramatically increased in Finland. It is estimated that there are currently 50-60 quick loan companies. Inadequate authentication of quick loan applicants has led to a number of cases where the loan has been taken in another person's name without them knowing about it.

In many of the quick loan companies, authentication of the loan applicant is based solely on the social security number given by the applicant and subscription data from the telecommunications company. If this data checks out, it is assumed that the applicant is who he/she claims. Inadequate authentication has led to identity theft. Authentication difficulties are complicated by the fact that specific obligation to identify the quick loan applicant has not been imposed on the creditor.

In March 2007, the Data Protection Ombudsman asked the competent Data Protection Board to order a quick loan company to change their authentication process pertaining to loan applicants. The Data Protection Ombudsman required that creditors identify their clients in order to ensure the accuracy of any personal data processed. The view of the Data Protection Board will have even more general significance, since according to a survey commissioned by the Data Protection Ombudsman, almost all businesses in the field use a similar system based on weak identification.
The decision may have repercussions on other fields of business as well.

*****

IRELAND

A number of Regulations were made in October 2007 in particular:
- Regulations to exempt certain categories of data controllers and processors from the requirement to register with the Data Protection Commissioner in line with the provisions in Directive 95/46/EC;
- Regulations to provide that the processing of genetic data in relation to the employment of a person can only take place with the prior approval of the Data Protection Commissioner.

*****

ITALY

Major Developments in the Data Protection Field

Law Enforcement Databases
The management of large databases for law enforcement purposes was one of the main focuses of attention for the Italian DPA also in 2007. In particular, the Authority also carried out in-depth investigations in respect of the processing of data by judicial offices. The need for applying more stringent security measures in this sector was pointed out – in particular by having regard to the exchanges of wiretapping records between telephone operators and judicial authorities. The lack of adequate arrangements in respect of the keeping and handling of personal information was confirmed, inter alia, by the inspections carried out at the Court of Rome, the largest one in Italy as for the volume of cases handled annually. The Authority continued its co-operation with the ministry of Justice, the national council of the judicature, and judicial authorities in order to enforce and facilitate compliance; the lack of sufficient financial resources should be referred to here as one of the main reasons for the difficulties encountered by the judicial sector in ensuring adequate safeguards to citizens' data.

Security in Telephone and Electronic Communications
Following an in-depth investigation into the processing of personal data by the main telecommunication operators in Italy, the Authority discovered abnormalities in the collection and processing of personal data related to use of the Internet. In particular, some operators acting as "internet access providers" were keeping detailed records of their users'/subscribers' web navigation, allegedly because they were obliged to do so by the law. To that end, various tools were used including hardware probes, transparent proxies and packet inspection techniques, which allowed collecting information with a detail level ranging from the source/destination IP address couple to fine-grained HTTP logs – up to search engine query-strings submitted by users, authentication credentials transmitted over simple HTTP connections and any sensitive information that can be specified in an URL-format web address.

This kind of processing is not justified by technical reasons as related to the tasks discharged by Internet access providers, which is why the Authority issued three provisions to ban the processing in question and ordered the providers to delete all the users'/subscribers' navigation data recorded unlawfully within sixty days. The Italian DPA also adopted a general provision regarding the storage and processing of traffic data produced by telephone and internet service providers. This was aimed at ensuring enhanced security in respect of the traffic data retained by providers for lawful reasons (including law enforcement purposes). The measures developed by the Garante clarify who is to retain which data and lay down technical and organisational arrangements to ensure secure storage of the data in question. In particular, it is clarified that Internet content providers, search engine managers, public bodies/organisations making available telephone and Internet networks to their staff and/or using servers made available by other entities, Internet cafés and similar establishments fall outside the scope of application of the retention obligations at issue – pursuant to the definitions set out in directive 2002/22/EC on universal service as well as in directives 2002/58/EC and 2006/24/EC. Several technical measures were set out in order to protect the data - including strong authentication and biometrics procedures, fine-grained audit applied to databases and computer systems, encryption of databases, centralized and securitized log collection, and physical security measures for the protection of computer rooms and data centres.

Formal Complaints

In 2007, there were 316 decisions on formal complaints. Like in previous years, most of them concerned banks, financial companies and credit reference agencies. A few cases related to processing of the so-called commercial information (assets and liabilities, bankruptcy/winding-up procedures, etc.) by companies operating in this sector; they resulted into decisions urging such companies to perform in-depth checks before re-using public information in order to ensure that the information in question was updated, accurate, and complete.

Several cases that addressed the processing of data for journalistic purposes enabled the DPA to probe deeper into the "personal data" concept. Regarding identifiability of data subjects, the data related to individuals who were not explicitly identified but could be recognised by reference to other items of information held by the data controller (or available elsewhere) was considered to be personal data; however, it was stressed that it was necessary to take account of all the means that could be reasonably used by the data controller and/or another entity to identify the person in question. Mention should also be made of a case in which the personal information published in respect of two individuals other than the complainant - whose husband had been reported to have deceased in a car accident while he was "with his current partner" - was considered to be personal data related, albeit indirectly, to the said complainant because it produced effects that also impacted on the complainant in question.

Interestingly, the DPA ruled that the complaint lodged against a hospital was inadmissible because the access request was not aimed at obtaining communication of a personal genetic data held by the hospital, but rather the delivery of a tissue sample related to the complainant's deceased father (in particular, a "tissue fragment included in paraffin" and/or a blood sample.)

Inspections

The inspection activities by the Garante were enhanced in 2007, partly on the basis of the six-month inspection plans developed by the DPA. In performing such inspections, the Garante can also avail itself of a specialised corps within the Financial Police (Guardia di Finanza), which was entrusted with checking compliance with the requirements concerning notification, information notices, security measures, and enforcement of the resolutions adopted by the Garante. Overall, 452 inspection proceedings were carried out. They mostly concerned private entities and were aimed at checking compliance with the main requirements laid down in the data protection legislation. In particular, the Inspection Department focused on the processing of personal (medical) data by pharmaceutical companies and health care bodies; the online processing of personal data; processing aimed at the provision of goods and services via distance selling mechanisms (including call centres); the processing operations performed by Revenue Offices; the retention of users'/subscribers' data by telecom operators; and e-banking services.

Following the inspections, 228 proceedings were instituted with a view to the imposition of administrative sanctions; in 15 cases criminal information was preferred to judicial authorities. Criminal infringements concerned non-compliance with resolutions adopted by the Garante; failure to take minimum security measures; and the violation of the prohibition against the remote monitoring of employees. The administrative sanctions imposed are expected to yield minimum revenues amounting to about Euro 725,000.
Mention should also be made of the specific activities carried out by the Italian DPA in pursuance of international agreements and conventions, especially those related to operation of the Schengen Information System and Eurodac databases.

Public sector

Biometrics. The DPA authorised a public body (office of the Superintendant for archaeological heritage) to use the hand contour in order to enable employees to access a high-security area. The biometrics-based system to be deployed by the office will only rely on the geometric features of the employees' hands without including any other biometric data. The hand contour will be associated with an encryption algorhythm and stored in the internal memory of the biometric equipment; the latter will only be operating in local mode by means of a digital keyword to be selected and entered by the individual employee. This processing was found by the DPA to be lawful and proportionate; whilst the hand contour information does not enable unique identification as is the case, for instance, with fingerprints, it is sufficiently detailed to be used in specific situations with a view to identity controls.

Employment Issues**.** Guidelines were issued in respect of the processing of employees' personal data in the public sector. The guidelines address the processing of public employees' medical data; the collection of fingerprints to access the workplace; and the dissemination of data on the Internet.
Local Authorities**.** The DPA issued Guidelines on the processing of personal data with a view to the publishing and dissemination of documents by local authorities. Specific safeguards were laid down in respect of the data related to individuals mentioned, e.g., in decisions and resolutions posted on the municipal bulletin board, in publicly available documents and/or in documents posted on the Internet, so as to take due account of the principle of transparency.
Schools. The DPA clarified that parents may film and take pictures of their children on the occasion of school theatricals, as the images in question are not intended for dissemination and are collected for personal purposes in order to be circulated among family members and friends. The DPA also provided guidance, in co-operation with the Ministry for education, on the use of videophones by students/pupils in schools.

Health Care

- The Italian DPA instructed local health care agencies not to include medical diagnosis information in the disability certificates they are required to issue for the applicants to be enrolled in unemployment lists and/or exempted from the payment of school/university taxes.
- Dissemination on the website of an Italian Region of the names related to 4,500 patients as well as of information on the respective health status was prohibited by the DPA.
- It was clarified that local municipal authorities may not request physicians to provide names and/or other items of information to identify the patients they visit at home.
- An inspection was ordered by the DPA and carried out with the help of the Financial Police following media reports on the presence of hundreds of medical records in a garbage dump. Information was preferred to judicial authorities against the relevant data controllers because of their failure to take minimum security measures.
- The DPA urged a public body to use payment order forms containing no references to the diseases affecting the respective beneficiaries, in particular HIV-related conditions; the inclusion of general wording and/or numerical codes was recommended.

A leaflet was published and disseminated ("Protecting Personal Data: Siding with the Patient") to raise citizens' awareness of the importance of data protection in processing operations performed by medical staff, health care bodies, and/or medical labs. It contains concise information on patients' data protection rights and the mechanisms to enforce them.

Processing of Genetic Data

Genetic data may only be processed in the cases provided for by ad-hoc authorisations granted by the Garante (after having consulted with the Minister for Health who shall seek, to that end, the opinion of the Higher Council for Health Care) and, as a rule, with the data subject's written consent.

The general authorisation issued by the Garante in February 2007 to enable this kind of processing filled in a major gap in the regulatory framework. It applies to several categories of data controller for purposes mainly consisting in the provision of health care and the performance of scientific research activities; the issue of genetic data used for facilitating family reunion was also tackled.

After defining the main concepts (genetic data, biological sample, genetic test), the authorisation lists the entities authorised to process genetic data for the purposes specified in the individual cases (health care practitioners, public and private health care bodies, medical genetics laboratories, natural and/or legal persons for scientific research purposes). The principle whereby genetic data may only be processed for such purposes if they are actually indispensable was re-affirmed along with the need for obtaining the data subject's written consent – the only exception being where genetic data are necessary to safeguard the genetic identity (with a view to reproductive choices, or treatment) of a third party belonging to the same genetic line as the data subject and consent may not be provided on specific grounds (legal incapacity, physical impairment, mental disability), or where statistical surveys are at issue or the research activity is provided for by law.

Data controllers must fulfil specific obligations, which are especially stringent as regards the contents of information notices. Genetic counselling is a mandatory requirement if the data are processed for health care or family reunion purposes, both before and during the genetic testing. Specific processing arrangements must be complied with and stringent security measures adopted – including encrypted storage and communication of genetic data and separation of identification from genetic data. The retention period of the data in question must not exceed what is absolutely indispensable for the specific purposes; no genetic data may be disseminated.

Private sector

A major effort was made by the Italian DPA in 2007 in order to simplify application of data protection legislation in the private sector.

Bulk Debt Transfers and Securitization

A decision (published in Italy's Official Journal of laws and regulations) allowed dealing with several applications lodged with the DPA for exempting data controllers from the obligation to provide information to data subjects in connection with bulk debt transfer and/or securitization. Such operations entail disclosure by the transferor to the transferee of personal data related to the debtors. Under the DP Code, the data controller may be exempted by the DPA from information obligations in specific cases, providing the processing at issue is publicized adequately – according to mechanisms to be set out by the DPA. The Italian DPA ruled that providing information to the individual data subjects (the debtors) entailed a disproportionate effort in this case and exempted the data controllers from the relevant obligations on two conditions: namely, an exhaustive information notice was to be published in the Official Journal no later than when the transfer took effect, and the debtors were to be provided with individual notices on the first useful occasion following the transfer (e.g. when sending the bank statement, or making a payment request) so as to inform them that the transferee had collected their personal data from third parties.

Guidelines for the Monitoring of E-Mail and Internet Usage

The DPA issued a general decision (dated 1 March 2007) applying to the monitoring of e-mail and the Internet carried out by public and private employers alike – in the light both of the case law of the EHRC (case of Copland v. UK) and the stance taken by the WP29. Pursuant to Italy's constitutional framework, employers are required to afford reasonable privacy to their employees in order to ensure that their personality can develop freely and without constraints. Given these assumptions, the guidelines in question attempted to reconcile the interests at stake by re-affirming, on the one hand, the employer's right to lay down the usage arrangements for the IT equipment committed to employees – including proportionate disciplinary measures – and, on the other hand, employees' right to be the subject of controls carried out in a stepwise, proportionate manner and be adequately informed about the processing of their data, which must be minimized. Specific recommendations and prohibitions were laid down in this framework – among the former, the need for employers to adopt an in-house policy tailored to the dimensions of the enterprise, and adequately inform their employees about the mechanisms for using email, the Internet and other electronic tools by also specifying whether and to what extent controls are carried out; as regards specifically the Internet, the categories of website considered relevant to the employment context should be specified, and configuration mechanisms and/or filters should be deployed to prevent certain operations (e.g. certain downloads); additionally, shared email accounts should be made available as well as an ad-hoc email account to allow receiving personal correspondence, whilst employees should be invited to designate a trusted third party (e.g. another employee) to access their mail and forward relevant messages in case they are away from work. The Authority prohibited any activity on the employer's part aimed to perform remote monitoring of employees; where such monitoring requirements are related to production, organisation and/or security in the workplace, the agreement of trade unions should be sought as provided for in other pieces of legislation. Based on the balancing of the interests at stake, the Authority decided that monitoring for preventative purposes may be carried out without the employee's consent also at an early stage, i.e. irrespective of the existence and/or the planned institution of a litigation, providing all the safeguards specified above are in place and the monitoring is proportionate to the specific context (e.g. on account of security risks).

Simplified Mechanisms to Ensure Data Protection in the Insurance Sector

The Italian DPA authorised insurance companies to implement a new, simplified procedure in order to inform customers on the processing of their personal data. Account was taken in this regard of the experience gathered over the past few years within the framework of the so-called "insurance chain", which includes several stakeholders such as joint insurers and re-insurance companies. In practice, it was decided that the information notice will have to be provided once and for all by the insurance company stipulating the contract with the individual customer. That company will be responsible for informing the customer about any subsequent and/or further use of his/her personal data – including the respective purposes and recipients – also on behalf of other entities in the "insurance chain", who often have no direct contacts with the data subjects even though they may process personal information after collecting it from the insurance company. Specific safeguards were laid down by the DPA in order to enable the companies to avail themselves of these simplified information mechanisms – in particular, the insurance company will have to inform customers about the entities processing their data in connection with the specific contracts; an updated list of those entities will have to be posted on the company's website, partly in order to facilitate exercise of access rights by data subjects; any purposes pursued by the companies/entities in question other than those related to risk management will have to be specified in the information notice; and specific consent requirements will have to be complied with whenever consent is actually necessary – which is often not the case, e.g. because the customer's data are indispensable to stipulate and/or enforce the contract. In particular, it was recalled that processing customers' data for marketing purposes requires ad-hoc consent, and that sensitive data (including medical information) may only be processed by insurance companies with the customers' written consent.

Practical Guidelines for SMEs

Practical guidelines were issued to take account of the specific needs applying to SMEs in respect of data protection issues. Starting from the consideration that certain requirements under personal data legislation are sometimes considered burdensome, in particular by SMEs, and in order to foster the view that data protection can turn into a major business asset as it can increase consumers' and users' trust, the Italian DPA issued the guidelines in question to provide SMEs with a tool that can facilitate compliance and highlight the simplification measures that are currently available. As well as clarifying the main obligations that apply to any entity processing personal data and basic data protection concepts (data controller/data processor; information notice; consent and mechanisms for ensuring it is informed, in particular when sensitive data are to be processed), the guidelines clearly set out in which cases the processing is to be notified to the Italian DPA and what security measures a company performing standard business activities is required to take. The options currently available for cross-border data flows were also described, including the use of standard contractual clauses, and a checklist was made available so as to enable a company to verify whether all the relevant steps were taken in view of ensuring compliance.

Media

Several issues were addressed in 2007 concerning data protection and journalism. As for the so-called court journalism, the DPA found that publication by some media of the transcripts (including wiretapping transcripts) from ongoing judicial investigations was in breach of DP legislation – in particular, because the transcripts contained personal data (some of them relating to sex life) and their dissemination was in breach of the principle whereby the published information must be "material in view of the public interest". This principle is actually also laid down in the Code of Practice for the processing of personal data by journalists. In other cases it was found that personal data had been collected in breach of fairness and lawfulness principles – e.g. because pictures had been taken intrusively, or because videos had been recorded unbeknownst to the data subjects; of note, the processing in question was also in breach of the fairness and transparency obligations set out in the journalists' Code of Practice mentioned above. In a case concerning publication of news reports on a lady deceased after a serious illness, in which excessive identifying information had been disclosed, the DPA found that the safeguards set out both in the DP Code and in the journalists' Code of Practice had been violated since they apply to the deceased as well. Reference should be made finally to the special protection afforded to children by the DP Code in connection with media and journalism; a code of practice (Charter of Treviso) was adopted a few years ago for this purpose by the Italian journalists' association and endorsed by the Italian DPA. Many cases concerned the publication of data that allowed identifying – unnecessarily – children involved in legal disputes (separation, divorce) and/or in criminal proceedings related to sexual abuse.

*****

LIECHTENSTEIN

The Schengen/Dublin agreements were signed by the Government at the end of February 2008.

Signature of both, the Additional Protocol to the Data Protection Convention as well as of the Cyber Crime Convention are under consideration.

The Data Protection Authority received a complaint of an expert in a Council of Europe Committee. This expert complained of the fact that personal details were published in her CV on the Internet site of the Council of Europe. This complaint was transmitted to the Secretariat of the Public and Private Law Unit of the Council of Europe.

The new Police Act entered into force.

LITHUANIA

1. Information on Recent Developments at National Level in the Data Protection Field.

On the 3rd of April 2007 Seimas of the Republic of Lithuania adopted an Amendment to the Law on Residents' Register, which established that data about the kin relationships under single request referring the concrete purpose of the personal data use, may be transferred to the law enforcement subjects in order to fulfil designated functions; to the Parliamentary commissions in order to fulfil the tasks designated by laws or Parliament resolutions. Such data may be also transferred to the Chief Official Ethics Commission to execute it's direct functions; to notaries – for the processing of inheritance cases, to check whether there are no restrictions imposed by law to conclude transactions with the close relatives; to person who according to the laws have power to decide questions on citizenship of the Republic of Lithuania – to take a decision related with the citizenship.

Draft Law on Electronic Communications was submitted to Seimas of the Republic of Lithuania by the Resolution No. 811 of 8th August 2007 of the Government of the Republic of Lithuania. This Draft Law was prepared in order to transpose Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC into national law. Draft Law on Electronic Communications foresees that traffic data of subscriber or registered user of electronic communications services may be stored no longer than 6 months from date of communication. If these data are necessary for entities of operational activities, pre-trial investigation institutions, public prosecutor, court or judge for the investigation, detection of criminal offences, undertakings providing electronic communications networks and (or) services have to store this information longer, but no longer than 6 months additionally by indication of authority authorised by the Government of the Republic of Lithuania - entity of operational activities. Data necessary to trace and identify the source of a communication, data necessary to identify the destination of a communication, data necessary to identify the date, time and duration of a communication, data necessary to identify the type of communication, data necessary to identify users' communication equipment or what purports to be their equipment, data necessary to identify the location of mobile communication equipment will be stored 12 months from date of communication. On 19th December 2007 the Draft Law was adopted by Seimas of the Republic of Lithuania, but the President of the Republic vetoed the adopted Draft Law and referred it back to Seimas for reconsideration. On 17th January 2008 Seimas again considered the Draft Law and did not adopt it.

State Data Protection Inspectorate issued sample Rules for Personal Data Processing at Schools, which were approved by the Order No 1T-45 of 4th of July 2007 of Inspectorate Director. The aim of Rules for Personal Data Processing at Schools – to regulate personal data processing at school in order to ensure the compliance and implementation of Law on Legal Protection of Personal Data of the Republic of Lithuania as well as other laws and legal acts governing the processing and protection of personal data.

On the 1st February 2008 Draft Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter – the Law) was adopted by the Seimas (Parliament) of the Republic of Lithuania. The amendments in the Law are the following: new regulation on video surveillance: the Law contains detailed provisions on purpose of the use of video surveillance, requirements for installation of video surveillance devices, notification to data subject, processing of collected video data, etc. The Law foresees new provision prohibiting the processing of personal identification number for the purposes of direct marketing; the provisions regulating processing of personal data for direct marketing were also supplemented; new article regulating data processing for the data for the purposes of ability – to-pay solvency. By this Law the position of the data protection officer was introduced.
The Law also introduces the procedure of the nomination of the Director of the State Data Protection Inspectorate. Director of the Inspectorate shall be civil servant. Director of the Inspectorate shall be nominated and dismissed by the Prime Minister of the Republic of Lithuania in accordance with the Law on Civil Service of the Republic of Lithuania. The term of office is five years. The same person may be nominated the Director of the Inspectorate for no more than two terms of office in turn. The Director of the Inspectorate must suspend his membership in a political party during his term of office. The legal status of the Director of the Inspectorate is designated by this Law and Law on Civil Service of the Republic of Lithuania. The Law foresees that Director of the Inspectorate may have deputies. The

Director of the Inspectorate shall, in his absence, be substituted by one of his deputies, who shall temporarily perform his functions.
The Law will enter into force on the 1st January 2009.

In 2007 State Data Protection Inspectorate celebrated its ten year anniversary. On this occasion on 15th of November 2007 the ten year activities of State Data Protection Inspectorate was presented to the public institutions of Lithuania, on 13-14th of November 2007 an International conference "Data Protection Tendencies in Information Society" took place. The conference focused the public attention to the rapid developments of information technologies, implacable onrush to Lithuania, positive aspect as well as the ways of preventing the increasing threats to individual's right to private life due to the processing of personal data. The danger to person's privacy induces greater interest of how to ensure data protection in this sphere. The presentations delivered at the conference dealt with the issues of personal identification in e-environment and providing e-government services; data retention according to the Directive 2006/24/EC and the implementation of this directive; personal privacy protection in publicizing courts' judgments and state institutions decisions; employees personal data and video surveillance data processing, other. At the conference the experience was shared not only by the mediators from Lithuanian public and private institutions but also by the data protection commissioners and representatives from data protection institutions abroad.

THE NETHERLANDS

Input of the Dutch Data Protection Authority
Compliance with the Dutch Data Protection Act is not only in the interest of individual citizens. Respect for individual privacy also serves a collective interest: a society in which we can assume that our personal data will not be misused, making it possible to trust the government, companies, institutions *and* each other.

In 2007, the Dutch Data protection Authority, College Bescherming Persoonsgegevens (CBP), has changed its strategic direction and has shifted priority to carrying out investigations and enforcement actions - the core task of any independent supervisory authority - to ensure a more effective promotion of the awareness of standards, and a stronger, more efficient enforcement of the compliance with legislation. Of course, enforcement action must be preceded by clarity on the standards underlying our action. In order to be able to achieve this change in course geared towards standards, investigation and enforcement, and given the budget allocated to us, we give priority, as regards requests for help and assistance, to serious violations of a structural nature and to violations which entail major consequences for a substantial number of citizens or for groups of citizens. Through the enrichment and broadening of general information on the Dutch DPA website, citizens are encouraged and helped to resolve their problems themselves and also, where necessary, to take action themselves.

In other words: as a supervisory authority, to exercise the maximum influence possible on compliance with the statutory provisions entrusted to our supervision, we started to intensify general information policy last year, putting citizens, professionals and organisations in a better position to be aware of and comply with (or ensure compliance with) their rights and obligations. We also started to give priority to the tasks falling upon an efficient and effective supervisory authority: investigating how compliance with the relevant statutory provisions is being observed and, when a violation is identified, taking enforcement action.

Large-scale data collection and processing was high on the agenda of the Dutch DPA in 2007, just as it has been in other years. At a national level, privacy problems in relation to the OV-chipkaart (digital transport pass) and the Elektronisch Patiëntendossier (electronic patient file) are salient issues. These and other subjects will be discussed briefly below in a selection from the activities undertaken in 2007.

Healthcare

The Dutch DPA issued a critical advice on a draft legislative proposal that provides for the introduction of an electronic patient file. In the opinion of the Dutch DPA, making patient files available to all care providers is far too risky, partly with a view to the protection required for particularly sensitive personal data. With the exception of emergency situations, only care providers with a treatment relationship with a patient ought to have access to the record in question. If this is not the case, there is a risk that unauthorised parties will misuse or misappropriate the medical data.

In 2007, the Dutch DPA also issued a negative advice on making the elektronisch kinddossier jeugdgezondheidzorg (electronic child record for the youth healthcare sector) compulsory in the legislative proposal that relates to youth healthcare and infectious diseases. The need for the central electronic storage of data had not been substantiated sufficiently. The Cabinet has since said that it is no longer seeking to create a central electronic child record and that it is looking for other ways to exchange communications in the youth healthcare sector.

Public administration

The BSN [citizens service number] was introduced at the end of November 2007. This marks the start of a new phase for the Dutch DPA. At the BSN management facility, a personal public service point will be created, which local authorities and citizens can approach with any questions they may have. As the authority responsible for supervision of the careful handling of personal data, the Dutch DPA is the authority with competence to intervene in the event of real problems with implementation of the Act.

The Dutch DPA also expressed its criticism of the proposal for a verwijsindex risicojongeren (VIR) (national reference index of young people at risk). The Dutch DPA agrees wholeheartedly with efforts to achieve better and faster help for children and young people with problems, but it is not yet clear whether the sole objective of the reference index is the provision of assistance, or whether its aim is also to help maintain public order. It is important for there to be complete clarity about key terms and criteria.

Police and the judicial authorities

Safety and privacy are both vital for citizens. However, all too often in public debate, these values are, rather simplistically, construed as opposing values. To help put the discussion back on course, the Dutch DPA, in collaboration with the Ministry of Justice and the Ministry of the Interior and Kingdom Relations, commissioned research into the identification of the most appropriate balance between the efforts to achieve a safe society and the efforts to safeguard the right to privacy. The resulting external research report, with guidelines for more effective dialogue, was presented at a symposium on 1 November 2007.

In situations where the police tap telephone calls in the context of criminal investigations, conversations between lawyers and their clients are often recorded too. These conversations with holders of confidential information entitled to privilege must be erased as soon as possible. A Dutch DPA investigation of the national wiretapping rooms shows that this does not happen correctly or on time in far from all cases. The Public Prosecution Service has announced that measures for the improvement of this situation will be implemented.

In recommendations on proposed new legislation, or other regulations in the field of criminal law, the Dutch DPA regularly raises the following question: has it been demonstrated that the regulations in question are really necessary? Is it clear that existing or previously proposed statutory possibilities fall short? For example, in the opinion of the Dutch DPA, in the light of improved identification possibilities in the future, the Minister of Justice has provided insufficient justification for the proposal for a central database for the storage of the identity of all suspects and convicted offenders. And do the plans by the police, the Public Prosecutions Department and the Koninklijke Marechaussee (KMar) [Royal Netherlands Military Constabulary] to record the registration number of all motorists entering Amsterdam via the Utrechtse brug, regardless of whether they have a clean record or not, really contribute to a safer society?

At the end of 2007, at the request of the Senate, the Dutch DPA issued advice on a legislative proposal that would extend the powers that the intelligence and security services, in their efforts to combat terrorism, have to obtain data on travelling, payment traffic and Internet use by citizens. The Dutch DPA believes that the need for these measures in addition to the many measures already in existence has not been demonstrated and considers that the consequences of this data analysis for individual citizens, but also for responsible parties and the services involved, have not (or not sufficiently) been recognised.

Trade and services

Following the announcement by the Dutch DPA that it would take enforcement action against the unlawful combined storage of the name and address details of travellers and their travel data, the public transport companies would seem to have finally recognised that the OV-chipkaart has side effects that are contrary to the Wbp. In 2007, in a pilot on the Amsterdam metro network, research was done into the impact of the card, which ended with the conclusion that the OV-chipkaart system is being used unlawfully. The Gemeentevervoerbedrijf (GVB) [Municipal Transport Authority] and other public transport companies have now undertaken to bring practice in line with the Wbp. In the technical design for data storage, a distinction will be made between name and address details on the one hand and travel movements on the other hand. As a result, the risk of the unlawful monitoring of individual people's travel behaviour will be limited considerably.

The Internet

Personal data are published on the Internet in a large number of different ways and are generally accessible worldwide, 24 hours a day, for an extensive and diverse public. There can be unexpectedly serious consequences for Internet users – amongst whom are many children – whose personal data are on the web. In 2007, the Dutch DPA developed and published guidelines in order to clarify what is permitted and what is not when publishing personal data on the Internet. The individuals responsible can use these guidelines to assess whether publication of personal data on the Internet is permitted. A large amount of information material has also been published on the Dutch DPA site. As regards minors, the Dutch DPA takes a proactive stance in providing the rules applicable for social networks and for online marketing.

The government also makes use of the Internet. In 2007, the Dutch DPA conducted an investigation into how the municipality of Nijmegen publishes data on planning permission. Complete scanned copies of application forms were published on the net, containing not only data on the property in question and on the alterations proposed, but also personal data on the applicant, including his/her signature. In the opinion of the Dutch DPA, the municipality must only publish compulsory data on the Internet – on the property in question and the alterations proposed.

The proper performance of a public-law task does not justify a situation where an administrative body automatically publishes all data on the Internet. The Dutch DPA will also publish guidelines on the privacy aspects of active public disclosure in the framework of the Wet openbaarheid van bestuur (Wob) [Government Information (Public Access) Act] in 2008.

Work and social security

Citizens do not automatically become suspects simply because they receive benefit or housing benefit. In the Waterproof project, old-age pensioners and recipients of a social assistance benefit in 65 municipalities in Friesland, Groningen and Drenthe were checked for fraud based on data on their water consumption and the water contamination surcharge. The data obtained were also used to check fraud with housing benefit. The Dutch DPA investigated this linking of computer files and ruled it unlawful. It is important to combat benefit fraud, but monitoring based on the linking of computer files is only permitted on the basis of sound risk analysis, since this makes it possible to show that it is necessary to further monitor a group of citizens at a high risk of entering the fraud zone. As a result of the Dutch DPA ruling, the Sociale Inlichtingen en Opsporingsdienst (SIOD) [Social Security and Investigation Service] is now working on the

development of risk analyses using Privacy Enhancing Technology (PET). In this way combating fraud and the protection of personal data seem to be able to go hand in hand.

Another way of uncovering benefit fraud is covert observation by social security investigators. The processing method used for the personal data connected with these activities has been laid down in a process description approved by the Dutch DPA. Research in 2006 showed that compliance with the obligation to inform citizens of the fact that they had been observed left something to be desired. The process description was then tightened up in 2007.

In the event of a transition to a occupational health and safety service provider, can the old service provider transfer employees' records to the new service provider without this being provided for by law? The Dutch DPA ruled 'no' in 2006. Further to indications from the field that this view caused problems, the Dutch DPA did research in 2007 to ascertain whether a different approach is possible within the existing statutory frameworks. This led to an outcome whereby transfers were made subject to a distinction between data that are not subject to medical professional secrecy and data that are. In the first case, the data may be transferred. In the second case, data may only be transferred under certain conditions.

*****

SLOVAK REPUBLIC

Implementation of Directive 95/46/EC

In January 2007 Personal data protection Office of the Slovak Republic (hereinafter referred as to the "Office") received a report from Directorate-General for Justice, Freedom and Security of the European Commission in which it was expressed that regarding the data protection the situation in the Slovak Republic is satisfactory. The Office executes his function in spite of limited financial as well as human resources.

Among still remaining and by the Act No. 428/2002 Coll. on protection of personal data as amended by latter provisions (hereinafter referred as to the "act on personal data protection") not exhaustingly covered issues belongs the performance of the Office´ activities in a fully independent manner. In view of the respective European experts the Office´s finances, competences and its constitutional incorporation are not on acceptable level yet. Those indicators of an independent performance hit mainly on the different prospects and visions of respective state administration officials and deputies dealing with budget allocation or deciding upon the status of institutions. Apart of that, there is also a need to execute several amendments of the act in order to achieve the full harmonization with data protection directive and consistency with new legal and technological developments as well.

The above mentioned issues will be subject of restatement of the act. This would be a long process which is as Office´s priority foreseen to be implemented in the year 2008.

Other legislative developments

Office within the "legislative proceedings on draft acts" commented 223 drafts acts, regulations and ordinances of the Government of the Slovak Republic. The most frequent drafts were proposals of Ministry of Interior, Ministry of Health and Ministry of Agriculture of the SR. This means a substantial increase not only in numbers but also in the general awareness of the state administration bodies involved in the national legislation process, particularly of their need to cooperate with national personal data protection supervisory authority more closely.

By the end of the year 2007 Directive 2006/24/EC (Data Retention Directive) has been implemented in the Slovak law as the amendment of the Act on Electronic Communications. The retention period concerning the operational, localization data and data on communicating parties

has been set up for 6 months in regards to the Internet communication data and for other types of communication 12 months.

Within the legislative activities relating to the preparation to Schengen accession partial amendments of a special act and a governmental decree have been provided and adopted, namely the amendment of the Act of Police Corps and of a decree of the Ministry of Interior. Office's proposal to designate Ministry of Interior to be the controller of the Schengen information system as well as controller of all other police information systems has been accepted. Passing this act an ultimate step for the successful inclusion of the Slovak republic to Schengen area has been conducted.

Major case law
In 2007 resumed two cases from the past years – in one of them Ministry of Justice of the Slovak Republic sued the Office for its decision from 2006 on unlawful publication of the national identification number (so called birth number) on the internet pages of the Commercial Bulletin. Office in accordance with the diction of the act on personal data protection ordered that all published birth numbers ought to be removed from the web or at least lapped. Ministry submitted an objection to the decision in line with the act which was turned down. The trial was brought up to the Supreme Court and was terminated by the denial of the claim of the Ministry by the end of January 2008.

In the latter the decision of the Regional Court of the Slovak Republic that defendant (Office) was legitimate to take actions against public disclosure of already published personal data on a website of one Slovak journal was confirmed by the verdict of the Supreme Court it means in favor of the Office.

Major specific issues
In the year 2007 filed data subjects and other natural persons alleging that their rights stipulated by data protection act were directly infringed 121 notifications to the Office. 27 notifications were filed by other subjects who announced suspicion of violation of data protection act. The chief inspector of the Office ordered 125 proceedings to be conducted ex offo. Together the Office dealt with 290 notifications in the year 2007. This fairly high number consisted also from cases unresolved as of the end 2006.

It is to mention that in 2007 the inspection department by controllers and processors of the information systems conducted altogether 102 inspections and 62 "submissions to explanation". In comparison with the year 2006 it was an increase by 65 percent. In the year 2006, for the effective removal of by the inspection ascertained shortcomings, 104 binding orders have been issued. Office controlled prevailingly camera systems, particularly by the city police.

In 2007 Office imposed 7 fines, whereby the sanctions fell in the lower bound of the fine scale.
In regards the preparations for the Schengen accession and following the provisions of the act on personal data protection obliging the controllers to give the data subjects by gathering of their personal data a detailed information on the processing the Office conducted inspection in the diplomatic representation bodies of the SR and their consular departments in Serbia (Beograd), Croatia (Zagreb), Ukraine (Uzhorod), Belarus (Minsk), Russian Federation (St. Petersburg) and Turkey (Ankara, Istanbul). The inspections were further performed in the Office of Border and Foreign Police of the Slovak Republic, Office for Criminalistics and Expertise – department of EURODAC and on the Customs Directorate of the Slovak Republic.

Swift case
Immediately after bursting out of the Swift affaire the Office asked for cooperation the National Bank of Slovakia. In view of its representatives the problem was blown-out and all respective concerns inappropriate. After issuing of the opinion of the WG29 on Swift in November 2006 the chief inspector of the Office summoned 24 bank institutions to complex evaluation of their policy relating to the transborder payment system performed among each other and via Swift. A special

consideration should have been given to the mandatory obligation of the banks to inform their clients about the conditions of the processing of their data and in this respect particularly about further disclosure of their personal data to legal subjects residing abroad. The investigation showed that some of the financial institutions do not utilise international transfers via SWIFT services or they do not have any contractual relationship with SWIFT or they provide financial services to corporate clients whereby the requirements of the act on personal data protection or Directive 95/46/EC are not applicable. The investigation further revealed that the clients of banks concerned are indeed not informed about the transfer of their personal data to Belgium and further to the USA on purpose of the fight against terrorism. Consequently, Office's representatives negotiated with the Slovak Banking Association and agreed with them on the elaboration of a uniform information notice for the clients concerning the personal data transfer via Swift. The information notice should have been incorporated into bank's data protection policies, put on the client desks in writing and published on the bank's web pages. The financial institutions were asked to comply with the agreed requirement on this specific client information notice by the end of May 2007.

Processing of personal data of clients of companies rendering funeral service
Office conducted inspections in information systems of various funeral service companies. The object was to examine if all services are performed and the personal data of their clients processed in compliance with the act on personal data protection. In all cases it has been proven that the respective controllers of information systems do not comply with Slovak data protection law in various aspects.

Special registration for biometric personal data
By conducting of an inspection in a company – famous producer of brand electronics it has been discovered that the controller did not register its information system containing biometric data. In coincidence with the act on personal data protection the controller is obliged to submit the information system to special registration if he intends or if is he already processing biometric data, except for analysis of DNA and the DNA profile of natural persons for the purposes of registration or identification in entering the sensitive, especially protected facilities, the premises with reserved access or in accessing technical appliances or devices with a high rate of risk and in the cases of solely internal needs of the controller. In this particular case the Office imposed fine in the total high of 30.000,-SKK.

Unlawful disclosure of personal data by non banking company providing credit loans
The company in question used to send to its debtors reminder letters whereby the letter was put in a correspondence letter of red color. The open form of such letter allows easily and transparently to see the personal data of the addressee, including their economic identity. Office interdicted the processing in above described manner because it was not objectively necessary for fulfillment of the original purpose of the processing of personal data.

Unlawful publication of national identification number ("birth number")
Office conducted inspections in the information systems of various public and private administration bodies as the Fiscal Directorate of the Slovak Republic, one football association, one ski club, Anti-trust Office and Governmental Office of the Slovak Republic. In all cases it has been proven that the controllers of the information systems do not comply with Slovak data protection law in various aspects.

Scanning and copying of documents without data subject's consent
Copying and scanning of documents cannot be performed without due legal cause, which is in Slovakia either a special act or written consent of a data subject. By the inspections performed in various public and private entities the Office was made sure of ignoring these rules by vast majority of controllers. They usually conducted this kind of processing over the extent necessary for achieving of the purpose of the very processing of personal data and without the due consent of data subjects. Office issued in this respect binding orders.

Transborder data flow
Within the Office's organizational structure the department of foreign relations is charged to dispose of all requests on international data transfers. In 2007 the department issued more then 30 official statements (explanations, interpretations of law) concerning transborder data flow within or outside the European Union. Under Slovak act on personal data protection controllers are obliged to seek approval of their international transfers of personal data by the Office solely in case of the transfer from controller in the Slovak republic to processors in third countries not ensuring an adequate level of personal data protection. Insofar the employment data are those mostly wanted among the categories of personal data transferred to the third parties abroad. However, the banks are requiring also some sensitive personal data, as national identification number, which seems to be excessive to their service performance and justify it by their globally interconnected and mirrored information system. The Office was asked for approval mainly by subjects of financial (banking) sector and those transfers were also approved (together 9 approvals). In other cases, largely incomplete grounds provided by the controllers seeking the Office's approval for the designed data transfers taking place all over the world led mostly to denials of approval. One approval has been issued for a global mobile operator in beginning of January 2008.

The application difficulties with the respective sections on transborder data flow of the act on personal data protection were aimed to be liquidated by the issuing of Guidelines for controllers concerning international transfers of personal data which were published on the Office´s web page by the occasion of the second Data Protection Day.

Public Opinion Poll
Public opinion poll focusing on level of awareness in matters of personal data protection was conducted by the Opinion Research Institute of the Statistical Office of the Slovak Republic. The poll revealed that more then a half of respondents (51%) is aware of their rights related to the protection of personal data. More then two fifths of the respondents indicated that they were not provided with all information concerning the processing of their personal data in advance. Almost nine of ten respondents have never used their data subject's legal rights and never asked for information concerning processing of their personal data. Roughly one of twenty respondents applied for correction of his/her personal data. About 36% of the respondents did not know about their right to disagree with the transfer of their data in other EU member state. More then two fifths of the respondents were afraid of misusing their data via Internet communication. Equally, more then two fifths of the respondents agreed with tapping of their phone calls in case one would be suspect of terrorist activity. Almost one fifth of the respondents agreed with tapping when approved by a judge. More then two fifths of the respondents agreed with Internet communication monitoring if a person is suspect of terrorist activity. One fifth of the respondents agreed with monitoring when approved by a judge.

International cooperation
On March 21st, 2007 the second evaluation mission Sch–Eval of the European Commission visited Slovakia. The Office was examined together with other relevant authorities.

The Office has proven capability to full performance of its competences to inspect police databases. Slovakia solemnly entered to Schengen area one minute after midnight on December 21st, 2007.

Within framework of building up partnership with central and eastern European data protection authorities, additionally to the annual Central and Eastern European Commissioners Conference taken place for 2007 in Zadar, two days negotiations were held with deputies of Romanian DPA in April 2007 in Bratislava, where main issues of personal data protection, including the conditions met and steps to be taken for full accession of the Slovak Republic to Schengen area, were discussed. In its end the both DPAs concluded an Agreement on Cooperation.

Within the international project aimed to create and enhance effectiveness of the activities of the Directorate for Personal Data Protection and Data protection Enforcement of the former republic

of Yugoslavia - Macedonia one employee from the Office's department of foreign relations as the short term expert for information technologies and security had participated in that project. In June of 2007 was that representative of the Office elected chairman of the Joint Customs Supervision Body for the Customs Information system.

*****

SLOVENIA

Established by the Information Commissioner Act (adopted in November 2005), the new independent body **Information Commissioner** started operating in the beginning of 2006. The new body has resumed the work of the former Commissioner for Access to Public Information and the Inspectorate for Personal Data Protection which had operated as the constituent body within the Ministry of Justice. A joint field of work and jurisdiction of the Information Commissioner both in the area of access to public information and personal data protection is comparable with that in other EU states.

The **concept of personal data protection** in the Republic of Slovenia is based on the provisions of Article 38 of the Constitution of the Republic of Slovenia which constitutes personal data protection as one of the constitutionally enshrined human rights and fundamental freedoms. Thus the protection of personal data is ensured by the Constitution that prohibits the use of personal data contrary to the legitimate purposes of their collection. Furthermore, the collection, processing, application, supervision, protection and confidentiality of personal data can only be regulated by statute-law (adopted by the national parliament). The data protection subjects are assured of access right and judicial protection.

By **The Personal Data Protection Act** adopted in July 2004 and amended in July 2007 a systemic regulation of personal data protection and harmonization of Directive 95/46/EC were accomplished. Through a detailed determination of rights, obligations, principles and measures for data controllers this law provides also a direct legal basis for personal data processing in such sectors as direct marketing, video surveillance, biometrics etc. thus partly constituting the so-called »sectoral law«. By the adoption of this law together with other laws regulating the processing of personal data in particular sectors the system of data protection in the Republic of Slovenia has been rounded up and brought in line with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ratified in 1994).

Being rather new authority the statistics about a two-year **Information Commissioner's work** significantly reflect this fact.

Inspection activities: In 2007, the Information Commissioner received **406** (179 in public and 227 in private sector) applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act; compared with **231** cases (88 public and 143 private sector) in 2006 the increase amounts to **76 %**. Most complaints pertained to disclosure of personal data (PD) to unauthorized users, unlawful or excessive collection of PD, illegal video surveillance, insufficient PD protection, unlawful publication of PD etc. Accordingly, a significant increase has been noted in the initiated administrative offence procedures: 133 cases in 2007 compared with 41 cases in previous year.

The number of requests for **written opinions and clarifications** received by Information Commissioner has also significantly increased from 616 in 2006 to 1144 in 2007 (or even compared with just 34 cases in 2005!). This undoubtedly reflects a growing public awareness of the right to privacy brought to effect by a modern Personal Data Protection Act and is, hopefully, also related to the transparent work and intensive public campaigning performed by the Information Commissioner.

Other activities: Since deciding on the admissibility of the intended introduction of **biometric measures** also falls within the competence of the Information Commissioner another

significantly growing trend is noted in the number of related applications (40 in 2007 compared with 15 in 2006). The increasing number is also the case in granting permits for the **connecting of filing systems**.

During its operation the Information Commissioner has lodged applications for a **constitutional review** of certain provisions of four statute-laws and contributed in the preparation of many different pieces of **national legislation** from the point of view of personal data protection.

Information Commissioner's **public awareness activities** are important part of its work performed through issuing of publications, press conferences and other co-operation with media, participating in conferences and seminars, collaboration with competent authorities or groups, providing advise by phone, permanently updating and upgrading its informative web site http://www.ip-rs.si, etc.

International co-operation activities of the Information Commissioner besides bilateral co-operation include participation in the Article 29 Working Party, JSB Europol, JSA Schengen, JSA Customs, EURODAC Supervision, and lately in T-PD.

*****

SPAIN

Recent Developments in the data protection field in Spain

1. Legislative developments

During 2007, the following regulations with an impact on data protection matters were approved:

a. Act 11/2007, dated 22 June, on electronic access by citizens to public services

The purpose of this Act is to enhance the use of electronic means in the government-to-citizen relationships, improving the universal accessibility to the information and services provided by the Public Administrations, and the interoperability between the different administrative bodies. It establishes that the availability of the use of this kind of means, in a secure and comprehensible way, is a right of the citizens, and a correlative obligation for the Administrations. The processing of data, as is natural, must respect the obligations and rights set down in the Spanish Data Protection Law, guaranteeing the use of the data obtained by electronic means for the precise purpose for which they have been sent to a specific administrative body.

As a result of this Act, the Official Spanish Gazette and other official journals will be published in electronic editions. Likewise, due to its nature of basic law, it is being developed by the Autonomous Communities (e.g. Decree 232/2007 of the Autonomous Community of the Basque Country, dated 18 December).

→ http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/12352(in Spanish)

b. Act 25/2007, dated 18 October, on retention of data relating to electronic communications and public communication networks

This Act, a transposition of the Directive 2006/24/EC, establishes the retention of data on electronic communications for twelve months, for public safety purposes. Information regarding unsuccessful calls and pre-paid cards shall also be stored. The transfer of this information to security forces shall be done following a court order and only to authorised agents.

→ http://www.boe.es/t/es/bases_datos/doc.php?coleccion=iberlex&id=2007/18243 (in Spanish)

c. Act 37/2007, dated 16 November, on re-use of public sector information

This Act transposes the Directive 2003/98/EC to the Spanish legislation. It applies to documents that the public sector could make accessible for re-use by citizens or companies, in

order to exploit the possibilities that this kind of information may allow, with a view to contribute to economic growth and job creation, and to increase the transparency of the public sector too. As the Directive lays down, this Act does not alter the obligations and rights set out in the Spanish Data Protection Law.

→ https://www.agpd.es/upload/English_Resources/reglamentolopd_en.pdf

d. Royal Decree 1720/2007, dated 21 December, which approves the Regulation implementing Organic Law 15/1999, on the Protection of Personal Data

The approval of this Regulation becomes a milestone in the Spanish Data Protection legislation. It intends to guarantee the necessary legal certainty in an area as sensitive for fundamental rights as that of data protection, consolidating the precedents settled by the Spanish Data Protection Agency. It also intends to resolve the most frequently asked questions, and problems with interpretation that may currently exist, paying particular attention to those that may be of greater significance. Comments and observations from the current authorities of the Autonomous Communities have been taken into account, as well as those of more than sixty entities and associations representing the rights and interests affected by this Regulation.

The Regulation expressly includes within its scope of application non-automated files and processing of data (on paper) and sets out specific criteria regarding their security measures. It also regulates the territorial scope of application, establishing that all processing is subject to this Regulation if Spanish legislation is applicable, according to the rules of Public International Law, or when means located in Spanish territory are used, unless only for transit purposes.

Of particular significance is the incorporation of the authorisation for the processing of data is necessary for the purposes of the legitimate interest pursued by data controller.

Similarly, it regulates a procedure for guaranteeing that any person may have full knowledge of the use of such data, before consenting to his data being collected and processed. In addition to this, of particular importance is the establishment of specific rules relating to the provision of consent by minors, which will demand the assistance of their parents or guardians when the child is less than 14 years old.

In the pursuit of better guarantee the right of persons to control the accuracy and use of their personal data, the data controller is expressly required to provide data subjects with a free and simple means of allowing them to exercise their right of access, rectification, erasure and objection. Along the same lines, it is prohibited to demand the data subject send registered letters or similar, or use telecommunication means that imply the payment of an additional charge. Finally, although the Regulation is not applicable to deceased persons, to avoid painful situations for their relatives it provides that they may inform the data controller of the death and request cancellation of the data.

The applicable rules to data processors are also regulated in detail. Another novelty is the establishment of a detailed system for processing regarding, on the one hand, to financial solvency and creditworthiness, and on the other, to advertising and commercial research activities, implementing the specific provisions contained in the Organic Law 15/1999.

Regarding international transfers of data, the Regulation establishes a systematic regime for them, acknowledging the possibility that the Director of the Spanish DPA may declare the existence of an adequate level of data protection in a country where such a Declaration by the European Union does not exist, clarifying the situations in which guarantees may be provided which permit authorisation of a transfer by the Director, and including the so-called “binding corporate rules” or internal codes of multinational groups of companies. Finally, the Regulation establishes the procedures that the Spanish Data Protection Agency should handle for the performance of its functions, and expands the duty of the Spanish Data Protection Agency to collaborate with the data protection authorities of the Autonomous Communities.

→http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2008/00979 (in Spanish)

e. Act 56/2007, dated 28 December, on measures to promote the Information Society

This Act establishes some novelties regarding to electronic billing and to contracting processes in electronic commerce, in order to ensure the relations between users and consumers, and the electronic services providers, who must guarantee the respect to the Spanish data protection legislation rules in their processing of data.

Additionally, the companies that provide some services with a special economic relevance should facilitate the exercise, by the data subject, of the rights of access, rectification, erasure and objection by electronic means.

→http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440 (in Spanish)

2. Major case law

1. Video-surveillance resolution

The Spanish Data Protection Agency began an ex-officio investigation into the capture and dissemination via YouTube of images of a street in Madrid, in order to clarify whether there had been a breach of the Spanish data protection legislation regarding the capture using video cameras and later dissemination through YouTube, possibly having committed serious or very serious breaches of the data protection rules, punishable with penalties of up to €600,000.

2. Internet Forums

The Spanish Data Protection Agency resolves that the right of erasure also applies over personal data published on an Internet forum, when the data subject is not a celebrity nor is involved in a relevant fact. The disclosure of personal data on the Internet is not always protected by the freedom of expression.

3. Emule

The Spanish Data Protection Agency imposed a penalty on the disclosure of personal data on the Internet through the file-sharing system "Emule". This is the first fine imposed by the Agency for using systems which permit the sharing and downloading of text, video or music files, among others, that are stored in the computers of other users. The Spanish DPA reminds the importance of the implementation of security measures such as firewalls, and of the careful selection of the directory containing the information that is going to be shared.

4. YouTube resolution

The Spanish Data Protection Agency began an ex-officio investigation into the capture and dissemination through YouTube of images of a disabled person, protecting the right of cancellation of the data subject's representative, before a possible very serious breach of the Spanish data protection rules by processing and later disseminating data images relating to the person's health.

5. Sentence of the Spanish High Court on Apostasy

The decision of the AEPD on the right of citizens not to appear in the Register of Baptisms and to exercise their right of erasure on these files was appealed by the Archbishop of Valencia before the National High Court. The decision of this body upheld that of the AEPD. The following aspects of this decision must be emphasised:

- Registers of Baptisms are deemed personal data files in the sense of the LOPD.
- Failure to cancel such data may constitute a breach of the principle of quality of data.

3. Major specific issues

1. Appearance of the Director of the Agency before the Lower House of the Parliament

In his annual speech, the Director of the Spanish DPA emphasised the recent proliferation of video-surveillance devices, not only by public authorities but mainly in the private sector, through the generalisation of camera-installation initiatives, for example, in owners' associations, commercial premises or transport services. Furthermore, he pointed out services such as "YouTube" which permit the global dissemination of images to all Internet users.

In his speech he also referred to the need to offer guarantees before the new risks arising from Internet services such as “search engines and e-mail services”, reminding that search engines must guarantee the effective exercise of the rights of access, rectification, cancellation and objection.

2. Declaration on search engines

In 2007, the Spanish Data Protection Agency published the report on its main observations, relating to the adaptation to Spanish data protection legislation, of the policies on the collection, conservation and use of personal data of Internet search engines. This report includes the main conclusions of the analysis, carried out on the effect these practices may have on the privacy of users of the search systems and other services offered by these companies.

Conclusions:

- Search engines must bring into line the storage time limits, minimizing the risks to the privacy of users.
- The information provided to users is complex and inefficient.
- Citizens have the right to erasure and to object to their data appearing as the result of carrying out a search

→https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/declaracion_aepd_buscadores_en.pdf

3. Ex-officio Sectorial Inspection in Colombia

This inspection was carried out on companies making international transfers of personal data for the provision of services related to Telemarketing or Customer Service centres. Key issues are the evolution and increase registered by the Spanish DPA over the last few years in requests for international data transfers, their destination countries and main purposes for which they are requested.

→https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/report_Inter_data_transfers_colombia_en.pdf

4. Co-operation with other European Countries

1. Bosnia and Herzegovina

Spanish Data Protection Agency participated as Junior Partner with the Czech Office for the Personal Data Protection in a Twinning Project with the Data Protection Commission of Bosnia and Herzegovina, implemented between February 2006 and March 2007.

2. Bulgaria

The Spanish DPA was selected, during 2006, to develop a Twinning Project in Bulgaria. It was financed by the European Union Phare programme, having a budget of €700.000, and has been organized in five components: legal analysis, institutional building, information systems, enforcement and awareness raisings. 72 experts of several countries, such as France, Finland, Italy, Netherlands, Portugal or the United Kingdom, and the European Data Protection Supervisor too, have participated in this Project during its 14 months long. All the programmed activities and all the settled goals have been reached, making possible that the Spanish DPA considers, at the conclusion of the project, that it was very successful.

5. Activities by Spain on the Latin America Data Protection Network

The year 2007 was a particularly active year within the scope of the Ibero-American Data Protection Network, established in 2003 as a result of the Spanish DPA initiative to promote the regulation of data protection in Ibero-America. The 5th Ibero-American Meeting took place in 2007 in Lisbon (Portugal). A seminar in Cartagena de Indias (Colombia) was also held in 2007, with the objective of creating a forum for debate and exchange of information. Guidelines were established to promote initiatives that permit the achievement of an adequate level of data protection in the countries comprising the Ibero-American Community, thus avoiding the current

obstacles to the free movement of personal data in such countries. As part of its commitment to these countries, the Spanish DPA welcomed representatives of Mexico, Chile and Uruguay to its headquarters; the latter were advised on their Data Protection Bill.

*****

THE "FORMER YUGOSLAV REPUBLIC OF MACEDONIA"

The right of personal data protection

In the Republic of Macedonia, the right of personal data protection, as one of the fundamental human rights and freedoms, is established in Article 18 of the Constitution of the Republic of Macedonia. The legal framework, which in essence is harmonized with the Directive 46/95/EC of the European Commission and Convention 108 of the Council of Europe, is determined by the adoption of the Law on personal data protection that came into force in February 2005.

From its establishment, the Directorate for personal data protection is dedicated to the development of the legislation and its compliance with the Directive 46/95/EC of the European Commission and Convention 108 of the Council of Europe and the Additional Protocol to the Convention 108.

In the performance of its key competencies, except of the legislation, the Directorate always follows the good practices of the DP Authorities of other countries.

Performance of the main competencies of the Directorate for Personal Data protection

Control over the legality of personal data processing and administrative supervision over personal data controllers

One of the main competencies that the Directorate continuously carries out is control over the legality of personal data processing and administrative supervision over the controllers i.e. the holders of personal data collections. (See also Annex 1)

Year	***Number of administrative supervisions***
2006	6
2007	45
2008 (continued from 2007)	27
2008 initiatives for new supervisions	5

The number of administrative supervisions that have been carried out has an upward tendency, due to the increased capacities for carrying out this function.

Institutions in the area of finance, telecommunications, social protection and other state bodies that have major personal data collections have been subject of supervision.

The intention of the Directorate was that through performance of administrative supervision during the transitional period, which lasted until December 19th, 2007 and was intended to give enough time to the controllers to adjust their procession operations to the standards proscribed by the Law on personal data protection, to review the current situation and to turn the attention of the controllers to the irregularities, but in an educative and preventive way. After the transitional period has expired the penal provisions of the Law on personal data protection came into full force.

Providing expert opinion and interpretations

Another important competency of the Directorate is providing expert opinions and interpretations in the area of personal data collections. The majority of these opinions were

regarding bylaws created by personal data controllers, questions by natural or legal persons, draft laws and international agreements as well as assessments if the conditions required for transfer of personal data to other countries are fulfilled. If there are indications for breaches of Law, the Directorate sends instructions. In 2007 the Directorate issued 16 instructions, and till 01.03.2008 were issued 2.

The Directorate is also opened for cooperation and in every day practice answers to the requests for opinions given by the phone calls from controllers and citizens.

The Directorate also respond to the requests for meetings with the controllers on which expert opinions are provided.

The Directorate is also included in the working groups for preparation of draft laws or amendments of the laws in different areas (See also Annex 2).

Year	***Opinions provided***
2006	40
2007	74
2008 (as of 01.03)	25

Complaints handling and request by citizens

The issue which the Directorate focused on the most was the complaints handling and requests filed by the citizens for the entrenchment of the violation of the right to personal data protection. The Directorate is legally bound to investigate whether there was misuse of personal data or not.

The Directorate acted in a timely manner and currently all the complaints and requests of citizens have been processed. This activity is largely dependent on the level of public awareness about the right of personal data protection and the possibility to practice that right. (See also Annex 3)

Year	***Complaints and requests***
2006	6
2007	24
2008 (as of 01.03)	14

Public awareness rising

Public awareness rising and informing the citizens about the right of personal data protection and privacy was and is a key imperative of the work of the Directorate The Directorate organized press conferences, interviews and reports in both, the press and the electronic media, as well as a number of meetings, workshops and roundtables for various target groups.

Year	***Media coverage***
2006	15
2007	65
2008 (as of 01.03)	51

Seminars for raising the public awareness for data protection in different sectors such as: insurance, media, telecommunication, bank sector, statistic, labour law, health and others, were organized last year in the framework of the Project for Technical assistance to the Establishment of the Directorate for personal data protection and Enforcement of the Data Protection Principles, an EU funded project, managed by EAR.

The Directorate organized five seminars in cooperation with Agency for supervision of fully funded pension insurance in different areas of Macedonia.

The Directorate within cooperation the NGO organized seminars for raising the public awareness for data protection. The seminars were organized both for the public and private sectors (governmental bodies, media, telecommunication companies, internet providers, banks, insurance companies etc). The issues of the seminars were the improvement of the implementation and application of the Personal Data Protection Law, Law on Free Access to Public Information[3] and Law on Safety of Classified Information[4] and the challenges of the Information and Communication Technologies (ICT) in the framework of implementation of the laws. Actual problems concerning the publication of the personal data on Internet, and interconnection between privacy, data protection and Internet were the most interesting issues for debate of concerning parties.

International cooperation

Last but not least, the Directorate is caring out international cooperation with foreign organizations and institutions in the area of personal data protection

The Directorate became a member of the Spring conference European data protection authorities, Conference of data protection authorities of the countries of Central and Eastern Europe., Consultative Committee for personal data protection of the Council of Europe and received status of observer in the Working Party 29 of the European Commission. In addition to the membership in international conferences and organizations, the Directorate is a regular participant to the meetings of groups for personal data protection in the area of telecommunications and the best practices in EU countries.

International cooperation became a priority since the establishment of the Directorate. Due to the fact that personal data protection was virtually unknown in Macedonia prior to the establishment of the Directorate, we had no other choice but to build the foundation of the Directorate upon the experiences of our counterparts from the other European countries.

Cooperation with the police sector

In 2006 the Directorate actively participated in the preparation of the provisions of the Law on police that refer to personal data protection with intention to ensure harmonization with the Directive 95/46 of EC and the Convention 108/81 of Council of Europe, as well as Recommendation 15(97) for personal data protection in the police sector of the Council of Europe.

Considering the fact that the Law on police completely entered into force on 11.11.2007, a real expectation is that the provisions that refer to personal data protection will be successfully implemented as well as the mechanism for supervision over the personal data processing in the police sector.

In the police sector the Directorate participates in the preparation for negotiations for the SELEC Convention for cooperation in the prevention of cross-border crime. It is expected that SELEC will be a regional organization much like the EUROPOL and will assist the law enforcement agencies of South-East Europe to actively cooperate in fighting serious crime.

The Directorate actively participated in projects on national visa system, projects for building information system for integrated border management, for introducing an one-stop system for import and export.

[3] Official Gazette of the Republic of Macedonia no.13/06
[4] Official Gazette of the Republic of Macedonia no.09/04

EUROPOL

The provisions referring to personal data protection in the Law on police and the amendments and modifications of article 4 of the Law on personal data protection (that provide that provisions of this law are applicable on matters of public safety and as well as for criminal procedures), are prerequisites to start the activities connected with the preparations for signing of the Operative agreement for cooperation with EUROPOL that is a higher level of cooperation after the Strategic agreement for cooperation with EUROPOL signed on 16.01.2007.

The Directorate also assisted the Ministry of Interior in the process of signing the operational agreement with EUROPOL, by preparing the answers to the questions by EUROPOL in the area of personal data protection.

EUROJUST

The Directorate for personal data protection participates in the activities supporting the start of negotiations for signing an Agreement for cooperation between Republic of Macedonia and EUROJUST that is a key institution of the EU for fighting organized crime, computer crime, cross-border crime as well as other serious forms of crime.

On the meeting held on July 9, 2007 in the Hague between the delegation from Republic of Macedonia, comprised of representatives of relevant Macedonian institutions the DIRECTORATE, Ministry of Justice, and the Collegium of EUROJUST, the representatives of EUROJUST expressed their optimism that if Republic of Macedonia makes the necessary changes in the Law on personal data protection, the agreement could be signed during 2008 that will be and a strong impetus for the European integration process.

The newly drafted Law on amendments and modifications of the Law on personal data protection (which is pending approval by the Parliament) was submitted to EUROJUST for comments and opinions. The remarks were taken into consideration and added to the amendments of the draft Law

Capacity building

From the establishment of the Directorate in June 2005 until the end of 2006, 11 new employments of civil servants have been realized respecting the principle of fair participation of minorities.

In 2007, three new employments have been realized (one person was transferred), therefore now the Directorate has 15 employees and 2 elected officials.

Capacity building of the Directorate is planed to be completed by 2010 with 50 employees.

Project implementation

The implementation of the project “Technical assistance to the creation of a Directorate for personal data protection and enforcement of the data protection principles“ lasted for 18 months (May 31st, 2006 – November 30th 2007). The implementation was realized through 5 components: legal support, IT support, capacity building of the Directorate, strengthening the organizational capacity of the Directorate and last but not least public awareness rising.

The Directorate has successfully cooperated with a number of other projects that have personal data protection as one of their goals.

Amendments and modifications to the Law on personal data protection

The initiative to adopt a Law on amendments and modifications to the Law on personal data protection (with a draft version of the Law) is in Parliamentary procedure.

The amendments and modifications are aimed at achieving:

- Full **harmonization** of the national legislation in this area with the legislation of the European Union, concretely with Directive 95/46/EC of the European Parliament and the Council of the European Union.;

- Expansion of the definition of “special categories of personal data” by adding **philosophical beliefs, genetic data and biometric data** to it;
- Expansion of the provisions of this Law to the processing of personal data for the purpose of **public** and **national security**, **defense of the country and criminal procedure**;
- Regulation of **video surveillance**;
- Strengthening of the **independence** of the Directorate;
- Simplification of **the procedure for the establishment of the existence of a violation to the right of personal data protection**. by abolishing the Commission in the Directorate. The decision on the establishment of the violation will now be in the hand of the Director, and an administrative dispute may be initiated against it in the Administrative Court;
- Simplification of the procedure for **registration of personal data collections** by the controllers;
- Simplification of the procedure for **transfer** of personal data to other countries;
- Introduction of **inspections**;
- Introduction of the principle of **technical neutrality of the provisions** of this law, which would mean that regardless of the development of technology, the provisions regulating the standards for security of personal data will be applicable;
- Exclusion of the application of part of the provisions of this Law for the purpose of **literary and artistic expression as well as professional journalism**, in accordance with the ethical rules of these professions;
- Acquiring the status of a **misdemeanor body** by the Directorate, meaning that a misdemeanor commission will be formed within the Directorate and it will have the power to carry out the misdemeanor procedure and issue fines and other types of misdemeanor sanctions, in accordance with the Law on misdemeanors[5].

The amendments and modifications to the Law on personal data protection are expected to be adopted in the first quarter of 2008.

Strategic planning

The Directorate enacted a Strategy for development for the period of 2007-2010. The Strategy is structured according to the purposes and the Programs. The activities are designed annually and every year a report with the expected/achieved results would be prepared and if necessary the Strategic plan will be modified for the next period.

The Strategic plan is attached with a document for the necessary new employments in the Directorate for the referred period according to the annual Programs as well as the financial implications for the new employments and the necessary trainings (respecting the obligation for fair participation of the communities).

In special sections of the Strategic plan the influence over the national regulative is elaborated, the necessary amendments and modifications that should be made in other sector regulations, the influence and significance of human resources, as well as the key parameters and terms for successful implementation of the Plan with established indicators for the successful assessment of the results and the planned structure reforms of the Directorate.

The Strategic Plan is complied with the NPAA in order to ensure coherency with the national requirements and association with the *acquis.*

The Strategic Plan is submitted to the Ministry of Finance in order to provide sufficient budget for the following year.

[5] „Official Gazette of the Republic of Macedonia“ No.62/2006

Changes of the Strategic plan are expected after the amendments and modifications of the Law on personal data protection are adopted. Changes will refer to the extension of the Directorate's competencies that will arise from the amendment of the Article 4.

*****

ANNEX 1

The most frequent violations of the Law on personal data protection that were established in the course of the administrative supervisions are:

- Retention of data after the purpose for their collection was achieved
- Personal data that are processed automatically are not deleted
- Personal data were given to other users without stating a provision in the contract for personal data protection
- Controllers had no internal regulation concerning technical and organizational measures for personal data protection,
- Excessive data
- Processing of special categories of personal data without legal basis
- Collecting personal data by questioners without stating which answers a r obligatory and which are not
- Inappropriate provision of consent for the use of personal data for commercial purposes
- Keeping of personal data in premises that are not physically protected from unauthorized access;

ANNEX 2

The majority of these opinions were regarding bylaws created by personal data controllers, questions by natural or legal persons, draft laws and international agreements in the area of:

- Fully Funded Pension Insurance
- Securities
- Banking and finance
- Statistics
- Labor and welfare
- Telecommunications
- Direct marketing
- Health protection
- Insurance
- Free access to information of public character
- Electronic commerce
- Defense
- Transfer of personal data
- Taxation
- Labor relations.

The Directorate was included in the few working groups for the preparation of following laws:

<u>Law on Protection of Patients' Rights</u>

The Directorate was actively participating in the preparation of the Draf Law on Protection of Patients' Rights. The draft law, originally prepared by the Ministry of Health, was amended in terms of respecting the right to privacy of the patients, as well as allowing them to perform an insight to their medical files and request rectifications, if it is justified.

ANNEX 3

The complaints and requests filed by citizens were mostly about:

- Unauthorized disclosure of the URNC

- Unauthorized publication of personal data on the Internet
- Unauthorized transfer of personal data from one controller to another
- Identity theft
- Unauthorized transfer of personal data to other state
- Unauthorized deletion of data from e-mail accounts

ANNEXE VIII – INFORMATION SUR LA JOURNÉE 2008 DE LA PROTECTION DES DONNÉES

Information given by member States on activities carried out on the occasion of the Data Protection Day[1]

CROATIA

Even though the right to the protection of personal data is constitutional rights issue, that is, one of the fundamental human rights and freedoms, only a relatively small number of citizens know about this fact.

The marking of the Day is targeted at promoting the protection of personal data, raising the awareness of citizens with regard to their right to personal data protection, as well as getting them acquainted with the purpose of the processing of their personal data.

At 26th January 2008 at the City Centre One, Jankomir 33, Zagreb the Agency employees adviced the citizens on their right to personal data protection, replyed to their enquiries, conduced a survey (questionnaire) on how much the citizens know about their rights, as well as distributed promotial material (brochures, leaflets, handouts).

At 28th January 2008 the round-table discussion was on mark the European Day of Personal Data Protection, organised by the Croatian Personal Data Protection Agency as well as „The Consumer“, the association for the protection of consumers in Croatia.

The European Day of Personal Data Protection in Croatia was marked by electronic media:
- the Croatian Television
- the Croatian Radio
- the Croatian Radio – Radio Sljeme
- the Radio 101
- the Open Radio

and also by newspapers:
-Vecernji list
-Jutarnji list
-Vijesnik
-Privredni tjednik
-Metro

*****

CYPRUS

For the European Data Protection Day on 28 January 2008, our Office organised the following activities:

1. A relevant poster was designed and distributed for display on premises of civil services, private organizations, municipalities, banks, companies, labour unions etc.

2. The Article 29 Resolution adopted on the 5th December was translated to Greek and published on the Office´s website.

3. On the 27th, 28th and 29th of January, after an agreement with the Department of Postal

[1] Further information available on : http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Data_Protection_Day_default.asp#TopOfPage

Services, all mail passing through certain major post offices was stamped with the message "28 of January- European Day for Personal Data Protection".

4. On the 28th of January:

- The Commissioner gave a press conference at the Press and Information Office, which was covered by media for television, radio and newspapers.
- The Commissioner appeared on the main TV stations.
- A relevant televised announcement was broadcast by the Cyprus Broadcasting Corporation on prime time.
- A message was broadcasted on several radio stations

5. Relevant articles were published in daily newspapers.

*****

CZECH REPUBLIC

Description of Educational Program

1. **Contents – detailed survey of topics:**

One lesson will be dedicated to the right to personal data protection within the framework of human rights and the Czech legislation.

The fundamental rights guaranteed both by the Constitution and the Charter of Fundamental Rights and Freedoms include the right to protection of private and family life. It will be explained in this context why personal data must be protected and how such protection is ensured, and what is the relation of the Personal Data Protection Act to the European legal rules (i.e. how and why the Czech legislation is harmonized with European law). In particular, it will be explained that personal data are a key to our privacy, which is one of the basic values of our civilization.

Explanation will also be provided with respect to the principles of personal data protection and the "balance principle", which ensures equilibrium between personal data protection and security (this aspect is important especially in relation to the topical issue of terrorism), as well as a balanced relation between the general Personal Data Protection Act and the special laws that also provide for personal data protection. In the interest of preserving civil rights, it is increasingly important to be able to enforce the right to privacy and to be aware of the fundamental legal provisions, on the basis of which this right can be exercised.

One lesson will be dedicated to the subject of personal data protection in schools. The Office has experience with personal data protection related to a number of areas where personal data are processed. Personal data are also processed in schools. Explanation of these issues will be based on the principles of personal data protection that must be maintained from the viewpoint of Personal Data Protection Act and from the viewpoint of protection of privacy. On the basis of their practical experience, the teachers will be able to raise questions related to situations which they must face up within their educational activities.

Two lessons will be dedicated to the possibilities of applying protection of personal data and privacy in the framework of specific subjects (for more details cf. section 5).

2. **Form:**

A lecture followed by a discussion with the lecturers concerning specific situations or issues.

3. **Educational goal:**

In relation to approval of the Personal Data Protection Act, No. 101/2000 Coll., and establishment of the Office for Personal Data Protection (hereinafter "the Office") in 2000, the media have been paying increased attention to the aspects of personal data protection as an extremely important part of rights of each individual. Although the general awareness of this

aspect is relatively high in the Czech Republic, also thanks to activities of the Office, almost no or very little attention has been paid to certain social groups in this respect. These groups undoubtedly include children and youth. However, in the near future, the current students of elementary and secondary schools will gradually become adults and bear the related political and economic responsibilities. Therefore, their knowledge of personal data protection must be continuously raised so as to ensure that this issue is not out of their interest at a time when they can affect the future of the society as a whole.

Schools are amongst the most important information channels whereby the students of elementary and secondary schools can be acquainted with the subject of personal data protection. However, information provided to the students within the subjects of basic social science, history, information and computer technology must be correct and also linked with specific examples of the practical situations involving protection of privacy and personal data. Therefore, the Office for Personal Data Protection has created an educational program in the framework of DVPP, whose aim is to prepare the teachers at elementary and secondary schools for topics in the area of personal data protection and enable their incorporation in the educational programs of individual schools.

4. **Number of hours + educational goal:**

A lecture consisting of 4 teaching hours

5. **Number of participants and specification of the target group of teachers:**

Approximatly 40 persons may participate in each workshop.

The Certificates will be given after a test concerning PDP.

The primary target group consists of teachers of the following subjects:

subject	specific educational goal related to the given subject
Czech language and literature	ability to perceive the concept of privacy and personal data protection in various time periods on the basis of a literary text or a work of art
basics of social sciences	personal data protection and protection of privacy in the context of human rights, law and psychology
history	development of opinions on human privacy, its value and establishment of personal data protection in various time periods within the development of the European civilization, influence of totalitarian regimes on the perception of protection of privacy
mathematics, information and computer technology	protection of personal data, their securing in automated processing – security within the Internet, principles of administration of computer technology with respect to data protection, danger of identity theft, modern equipment in personal data protection (tapping, RFID, database systems), principle of electronic signature
biology	possibilities of taking DNA samples, their subsequent processing for verification or identification purposes, different approaches to DNA databases in other countries, creation of databases of fingerprints and other personal identifiers, sensitive data in health care; human privacy – privacy of animals

La Journée de la protection des données personnelles 2008

Le Bureau de la protection des données personnelles, République Tchèque, a organisé le 28. janvier 2008 le seminaire au Sénat du Parlement tchèque avec la participation de M.Graham Suttton.

Le 29 janvier 2008 pendant la conférence de presse du Bureau, le concours pour les enfants et jeunes „Ma vie privée! Ne pas regarder, ne pas renifler!“ a été annoncé. Le concours de dessin et d´essai sera fermé le 15 mars.

Le concours est soutenu par la Radio Prague, le web pour les enfants „Alik“ et par le Festival des films pour les enfants et jeunes gens de Zlin; les prix seront remis pendant la rencontre des enfants le 1er juin a Zlin - avec la participation de la télévision et de la radio.

Du 1er avril jusqu´au 1er juin, les travaux des enfants seront exposés dans „le train cinématographique“ qui traverse la République tchèque et la Slovaquie (organisé par le Festival). Nous organisons pendant ce voyage quelques rencontres avec des enfants consacrées au problème de la vie privée. Nos collegue slovaque pense se joindre à nous.

Parmi les participants du concours, citons aussi les enfants des „SOS villages“ de République Tchèque, Lituanie, Lettonie, Russie, du Kazachstan et de l´Ukraine.

Nous développons le programme de l´education pour les instituteurs et autres pédagogues, qui a obtenu l´accréditation du Ministere des Ecoles, de la Jeunesse et du Sport tchèque. Nous organisons des séminaires à travers tout le territoire.

Le programme pour les séniors est dévéloppé avec la Faculté de Médecine de l´Université Charles. Au mois de mars (le 8) nous participons au festival pour les séniors à Prague.

*****

ESTONIA

The most significant event which took place in relation to the Data Protection Day 2008 in Estonia was the conference “Data Protection and Media”. The main reason for choosing this topic was the new redaction of the Estonian Personal Data Protection Act which included the provision on media and which came into force at the beginning of this year. The new provision enacts the disclosure of personal data in case of the public interest and without data subject’s consent. In the discussion, over the issues on media and data protection, participated several legislators, journalists, prosecutors, PR-persons and data protection officials.

Due to the currently actual issues on media and data protection, the attention to the data protection area was also much higher in the nationwide and local press.

FRANCE

61% des Français pensent que la constitution de fichiers porte atteinte à leur vie privée

Les Français veulent davantage se protéger

Le 28 janvier, le Conseil de l'Europe célèbre la journée européenne dédiée à la protection des données personnelles et de la vie privée. Ce rendez-vous permet d'appeler l'attention des citoyens sur les risques liés à certains usages des technologies d'information et de communication qui font partie de notre vie quotidienne. A cette occasion, la CNIL, qui fête cette année ses 30 ans, rend publics les résultats d'un sondage qui souligne à la fois l'accroissement de sa notoriété auprès des Français mais aussi leur perception de l'atteinte à leur vie privée. Les tendances ainsi observées sont confortées par d'autres études qui soulignent l'importance croissante de la dimension « protection des données personnelles et de la vie privée».

Les questions de protection des données personnelles sont aujourd'hui au centre de la vie quotidienne : au travail, dans les relations avec les autorités publiques, dans le domaine médical, lorsque l'on voyage ou surfe sur internet, lorsque l'on consomme, etc. Tous ces actes impliquent la collecte d'informations personnelles pour alimenter des fichiers toujours plus nombreux.

L'objectif de la journée européenne de la protection des données, conformément aux missions de la CNIL, est précisément de faire prendre conscience à chacun qu'il est titulaire d'un **droit fondamental à la protection de ses données et de sa vie privée**. La défense de ce droit individuel, désormais reconnu au même titre que la liberté de la presse ou la liberté d'aller et venir, appelle une vigilance constante de tous.

Afin de mesurer la notoriété de la CNIL auprès des Français, ainsi que leur connaissance de leurs droits à la protection des données personnelles, **TNS Sofres** a réalisé fin 2007 un sondage en face-à-face auprès d'un échantillon de 1000 personnes représentatif de l'ensemble de la population âgée de 18 ans et plus.

- **50% des personnes interrogées connaissent la CNIL, soit 11 % de plus qu'en 2006, et 16% de plus qu'en 2004.**

Depuis 2004, la CNIL a renforcé sa politique de communication, avec une présence régulière dans la presse pour mettre en avant la grande diversité des sujets qu'elle expertise et expliquer les nouvelles règles issues de la réforme de la loi d'août 2004. C'est grâce à cette présence médiatique constante que la notoriété de la CNIL passe le seuil des 50 %, trente ans après sa création.

- **61% des personnes interrogées estiment que la constitution de fichiers porte atteinte à leur vie privée**
- **26 % des personnes interrogées ont le sentiment d'être suffisamment informés de leurs droits à la protection des données personnelles**

Alors même que 61% des Français sont préoccupés par la constitution de fichiers, on constate toujours leur insuffisante connaissance des droits (seulement 26% des Français).

Ces résultats se confirment également dans le **« Baromètre de l'intrusion ©» réalisé par l'Agence marketing services ETO** qui relève que **76% des internautes se disent gênés par le fait que de nombreuses informations les concernant soient stockées dans des fichiers et que 61% estiment être insuffisamment informés de leur utilisation**. De tels constats incitent les marques à privilégier des relations transparentes et non intrusives pour fidéliser leurs clients et instaurer des relations commerciales consensuelles.

23% des personnes interrogées par le CREDOC pour l'enquête annuelle sur la diffusion des technologies de l'information à l'initiative de **l'ARCEP et du CGTI**, estiment que **les données personnelles sont insuffisamment protégées sur internet**. Cette protection insuffisante est citée par près d'une personne sur quatre comme le **principal frein à l'utilisation d'Internet**.

Afin de sensibiliser le plus grand nombre à ces droits, il est maintenant urgent de pouvoir mener, avec le soutien des pouvoirs publics, des campagnes d'information à destination du grand public et notamment des plus jeunes. En effet, il est nécessaire de s'assurer que le développement des nouvelles technologies de l'information s'accompagne d'une prise de conscience des droits à la protection des données personnelles et d'une auto-vigilance de chacun. La CNIL, en l'état actuel de son budget, et malgré les efforts significatifs récemment consentis par le gouvernement, ne peut mener seule cette mission ambitieuse. Les 15 *Rencontres Régionales* de la CNIL organisées depuis 2005 participent à cette campagne d'information auprès des organismes publics ou privés. Ces rencontres précèdent la création prochaine d'antennes régionales, si le budget accordé à la CNIL le permet. Les 2000 organismes ayant désigné un correspondant informatique et libertés participent également à la diffusion quotidienne d'une culture « informatique et libertés » qui garantit le respect des droits de leurs salariés et de leurs clients.

SOURCES

Sondage TNS Sofres réalisé pour la CNIL les 7 et 8 novembre 2007 auprès d'un échantillon national de 1000 personnes représentatif de l'ensemble de la population âgée de 18 ans et plus, interrogées en face-à-face à leur domicile par le réseau des enquêteurs TNS Sofres.

L'Agence ETO a réalisé le Baromètre de l'intrusion© du 22/02/2007 au 19/03/2007 auprès de 35413 internautes, grâce à la participation de 10 enseignes partenaires et du cabinet d'études Market Audit.

Le Conseil Général des Technologies de l'Information (CGTI) et l'Autorité de régulation des communications électroniques et des postes (ARCEP) ont confié au CREDOC la 7ème enquête annuelle sur la diffusion des technologies de l'information dans la société française.
L'enquête de juin 2007 a été réalisée auprès de deux échantillons distincts, représentatifs, sélectionnés selon la méthode des quotas. Le premier porte sur 2015 personnes de 18 ans et plus, le second sur 215 individus âgés de 12 à 17 ans. Toutes les interviews se sont déroulées « en face à face », à domicile.

http://www.cnil.fr

IRELAND

The Minister for Education and Science and the Data Protection Commissioner launched a new educational resource on privacy and data protection for secondary schools. It was produced by the Office of the Data Protection Commissioner in conjunction with the Curriculum Development Unit of the Department of Education and Science as a resource for schools to draw upon primarily in the Civic, Social and Political Education Course but also for integration as desired into other subjects. It is being distributed to all secondary schools nationwide. Further information in relation to this initiative is available on the Data Protection Commissioner's website: http://www.dataprotection.ie.

The Office of the Data Protection Commissioner, in association with Youtube, launched a video clip competition on the theme of 'privacy in the 21st Century'. This on-line competition is being run on Youtube and is targeted at young people. Further information on the competition is available on the following website: www.youtube.com/privacycomp.

LIECHSTENSTEIN

Pressemitteilung zum Datenschutztag vom 28. Januar 2008

Im April 2006 beschloss das Ministerkomitee des Europarates, jedes Jahr einen Datenschutztag durchzuführen. Zweck dieses Tages, welcher in den Mitgliedsstaaten des Europarates abgehalten wird, ist die Sensibilisierung der Bevölkerung für den Schutz der Privatsphäre. Am 28. Januar 2008 findet der 2. Europäische Tag des Datenschutzes statt, welcher erstmals auch in Liechtenstein durchgeführt wird.

In einer Resolution zum Datenschutztag bezeichnet die so genannte Artikel 29 Arbeitsgruppe, ein Gremium unabhängiger Datenschutzbehörden des EWR-Raumes, den Schutz der Privatsphäre als Lebensnerv unserer modernen Informationsgesellschaft. Ein gläserner Bürger sei unter keinen Umständen vereinbar mit der Menschenwürde.

In einer zunehmend vernetzten Welt nimmt die Kommunikation einen zentralen Stellenwert ein. Damit verbunden ist auch der Austausch von Personendaten, sei es telefonisch oder z.B. per Email, in sozialen Netzwerken oder allgemein auf dem Internet. Verschiedene Datenschutzgremien in Europa befassen sich 2008 verstärkt mit Fragen um das Internet, welches etliche Missbrauchsmöglichkeiten mit sich bringt. Eine weitere grosse Herausforderung stellt insbesondere der sehr wichtige Kampf gegen den Terrorismus dar, der jedoch nicht dazu führen darf, dass die Rechte der Bevölkerung ausgehöhlt werden. Zu nennen sind hier beispielsweise: die europaweite Pflicht zur Einführung einer verdachtslosen Vorratsdatenspeicherung im Telekommunikationsbereich und die damit verbundene heftige Diskussion z.B. in Deutschland, die Einführung von biometrischen Pässen, die Übermittlung von Flugpassagierdaten in die USA oder die Kontrollmöglichkeit von internationalen Finanztransaktionen durch US-Behörden, bekannt als SWIFT-Affäre.

Dem Datenschutzbeauftragten Liechtensteins ist es ebenso ein Anliegen, die Öffentlichkeit verstärkt für Belange des Schutzes der Privatsphäre zu sensibilisieren. Dies nicht nur im Zusammenhang mit dem Internet, zu dem bereits zahlreiche Informationen auf der Internetseite www.sds.llv.li zu finden sind. Der Datenschutzbeauftragte lädt die Öffentlichkeit daher ein, ihre Rechte, sei es Auskunfts-, Sperr- oder Löschungsrecht, vermehrt zu nutzen. So kann z.B. jeder einzelne Betroffene die Zusendung unerwünschter Werbung unterbinden oder die Löschung falscher Angaben über die eigene Person verlangen. Sollte beispielsweise der eigene Name unerwünscht auf einer Internetseite auftauchen, besteht das gesetzliche Recht auf Löschung desselben - und dies nicht nur in Liechtenstein, sondern in ganz Europa. Mit dem Auskunftsrecht besteht die Möglichkeit, Auskunft darüber zu erhalten, welche Angaben zur eigenen Person vorhanden sind. Dies gilt z.B. bei einem Unternehmen bei dem keine Gewissheit besteht, dass Daten bearbeitet werden oder mit dem seit Jahren kein Kontakt mehr besteht. Musterbriefe zur Geltendmachung der gesetzlichen Rechte sind auf der oben genannten Internetseite unter der Rubrik „Onlineschalter" abrufbar.

Aus Anlass des diesjährigen Datenschutztages hat der Datenschutzbeauftragte *Richtlinien für die Bearbeitung von Personendaten im privaten Bereich* herausgegeben. Diese Richtlinien sollen insbesondere Unternehmen über eine richtige Bearbeitung von Personendaten, zum Beispiel bei einer Datenbekanntgabe ins Ausland, informieren. Ausserdem wurden die *Richtlinien über die Rechte der betroffenen Personen* aktualisiert und neue *Richtlinien über den Umgang mit unerwünschter Werbung, insbesondere mit Spam* veröffentlicht. Die Richtlinien können alle übers Internet abgerufen oder aber direkt bei der Stabsstelle für Datenschutz bezogen werden.

LITHUANIA

2. Information on the Second Data Protection Day.

The second European Data Protection Day was celebrated in Lithuania. The State Data Protection Inspectorate jointly with the Committee on Human Rights of Seimas of the Republic of Lithuania organized a conference "European Data Protection Day for Youth". The venue took place in the Constitutional Hall of Seimas of the Republic of Lithuania on 23rd January 2008. The event was on the occasion of the European Data Protection Day, traditionally celebrated on January 28th. Europe started to celebrate this Day on the initiative of the European Council which was supported also by the European Commission. On this day the European countries are invited to organize events dedicated to the personal data protection issues with the aim to let more and more persons know their rights in this field. This year it is for the second time that the Day is celebrated. The objective of the event of this year was to draw attention of Lithuania's youth and introduce to them such important issues concerning each person as human rights. For the organizers of the venue it was important to find out what Lithuanian schoolchildren know about human rights, data protection, what topics relevant to the issues are posing certain concern to them. On behalf of schoolchildren of Lithuania some ideas were shared by the representatives of Lithuanian Schoolchildren Parliament. The event gathered nearly 80 schoolchildren of 14 to 18 years of age from Vilnius schools and colleges. The flyers were distributed to them which included thorough information on how safely to use internet and also other handout information material.

*****

ROMANIA

The National Supervisory Authority for Personal Data Processing has organized the following activities in order to celebrate the European Data Protection Day on the 28th January 2008:

a) In order to allow citizens to become familiarized with the field of personal data protection the **Open Doors' Day** has been organized in Bucharest on the 26th January 2008.

b) On the 28th January 2008 a **Public Debate on "the European Data Protection Day"** was organized in Tg. Jiu, Gorj county; the discussions were led by Mrs. Georgeta Basarabescu – president of the NSAPDP and the event was attended by important representatives of the local and central public authorities and institutions, members of the academic and university mediums, certain private companies and media.

The event gathered representatives of the Romanian Parliament – the Chamber of Deputies, of the Legislative Council, the Ministry of Communications and Information Technology, the Ministry of the Interior and Administrative Reform, Bucharest's Tribunal, Gorj County Prefect's Office, the General Romanian Police Inspectorate, the Gorj, Dolj, Hunedoara, Dâmbovița, Prahova, Suceava, Braşov, Mehedinți County Police Inspectorates and the Gorj County Council.

Moreover, on the occasion of the European Data Protection Day, representatives of the Hyperion University of Bucharest and the Simion Bărnuțiu Law School in Sibiu, institutions that have indicated great interest in the field of data protection, have addressed special messages to the Supervisory Authority in order to mark this important event.

The event was organized in Târgu Jiu at the initiative of the Gorj County Police Inspectorate and the Office of the Gorj County Prefect.

The reunion was opened by Chief Inspector Constantin Nicolescu – head of the Gorj County Police Inspectorate, as he underlined the specific goal of this meeting: to increase citizens'

awareness with regard to their rights referring to the protection of their personal data. Even though this is quite a new field in Romania the need to correctly implement the EU legislation was highlighted. Mrs. Georgeta Basarabescu expressed her gratitude for this initiative and the support given by county authorities in organizing the second celebration of the European Data Protection Day Târgu-Jiu, after the celebrations held in 2007 in Sibiu – the European Cultural Capital in honor of this important event, celebrated in all Member States of the Council of Europe.

In her speech, the Supervisory Authority's president underlined the fact that the Authority has begun its third year of activity, after passing in 2007 from the national level, in the field of data protection, to the European one, by fully implementing the European Union's standards. Mention was also made of the fact that in 2007 Romania was ranked 2nd place within the best results achieved in the field of data protection in a Report of *Privacy International*, issued in London.
Within this context some of the Supervisory Authority's achievements were mentioned, amongst which the initiative to issue an Emergency Ordinance which abolished the notification fees paid by data controllers, as this was considered to infringe on the free movement of personal data within the European Union member states.

In order to correctly enforce the provisions of the community's acquis, those of Law no. 677/2001 and improve the specific activities seven Decisions were also published in the Romanian Official Journal; mention should be made here of Decision no. 105/2007 on personal data processing carried out within credit bureau type filling systems. In issuing this Decision careful consideration was given to the risks to the private life of individuals involved by the automatic processing of personal data as certain aspects of their personality (such as behavior or credit worthiness) are scrutinized.

The event was also attended by Mr. Ştefan Marian Popescu Bejat – the Gorj County Prefect who expressed his satisfaction for hosting the European Data Protection Day in Tg. Jiu, as this proved to have been an excellent opportunity to increase awareness amongst citizens with regard to the principles of personal data processing, with the media's support.

Afterwards, a speech was held by Mr. Ion Călinoiu- president of the Gorj County Council, in which he highlighted the concept of interaction between public authorities and citizens which implies the processing of personal data and, implicitly, requires adequate information of the individual. Ensuring an adequate protection for personal data becomes an indispensable component of modern society.

Another important speaker was Chief Commissioner Dragomiroiu Gheorghe – deputy of the General Romanian Police Inspectorate and he gave a brief presentation of the excellent collaboration between the Supervisory Authority and the Romanian General Police Inspectorate from the point of view of training policemen in the field of personal data, especially in view of the envisioned adhesion to the Schengen area.

In his speech, Mr. Constantin Teodorescu – state secretary within the Ministry of Communications and Information Technology underlined the fact that the Draft legislative Act on the retention of traffic data is currently in the final stages of adoption by the Government and this regulation will extend the scope of the Supervisory Authority's competence. Mention was also made of nowadays rapid development of information systems and the increasing risks they involve with regard to the processing of personal data. this is why one of the measures foreseen for the e-governance project is that of citizens' authentification via Open-ID mechanisms.

The President of the IIIrd Section of Official Legislative Records within the Legislative Council, Mr. prof. univ. Sorin Popescu has underlined the importance of Convention 108 of 1981 which established the need to protect the individual's rights with regard to the automatic processing of personal data within today's society. The particcipants' attention was also

drawn to the fact that celebrating the European Data Protection Day was based on the 2003 which indicated a low degree of awareness with regard to personal data amongst citizens.

The discussions continued with the speechs of Mr. Sorin Goran – president of the Romanian Direct Marketing Association and Mr. Mihai Petroff – the Director of "Mailers", who underlined the interferences between the field of personal data protection and the activities of direct marketing companies as well as the involvement of the Supervisory Authority as early as 2006 in the specific issues posed by personal data processing in this field.

Mr. Ionel Condor – Director of « Ro Planet S.R.L. » brought to the participants' attention the IT sollutions which may be adopted by public authorities in order to manage their document flows and mention was made of the advantages brought by the system which has already been introduced within the Supervisory Authority.

These speeches have clearly shown the private companies' interest in correctly implementing the legal framework on personal data protection and the active role of the Supervisory Authority in increasing awareness with regard to the conditions under which personal data may be processed.

Mrs. Mihaela Muraru Mandrea has forwarded the message of the Parliament's Committee for European affairs, which highlighted the Supervisory Authority's activities in its 2 years' existence, the authority's important role in issuing specific regulation such as abolishing the notification fees, as well as all the other issues referred to in its Decisions.

Mr. Ion Stoica – head of the Dolj County Police Inspectorate has underlined the police's active role in training its staff, at all levels, with the specialist support of the Supervisory Authority's staff, as well as the need to continue the measures to increase awareness amongst citizens with regard to this field of activity.

The event ended with a Mr. Adrian Şuțu's display of caricatures on "data protection" at the premises of the Office of the Gorj County Prefect.

The reunion benefited from a large attendance of representatives of newspapers, TV and Radio stations; interviews were given for Tv Alpha Tg. Jiu, TV Antena, Radio România Actualități şi Radio Oltenia.

The large number of participants, the media's interest and the way in which it presented the field of data protection all lead us to believe that the event has reached its goal and the relevant information has been sent to the citizens.

c) On the same day, following the invitation of Chief Commissioner Constantin Nicolescu – head of the Gorj County Police Inspectorate, another **Debate on "Personal Data Protection within the National SIS**" was organized at the premises of the Gorj County Police Inspectorate with the participation of approximately 100 county police officers.

Within this reunion, Mrs. Georgeta Basarabescu – the Supervisory Authority's president has cleared up specific issues referring to personal data processing within the NSIS (the national component of the Schengen Information System).

The discussions continued on the measures which will be adopted in preparation of the Schengen evaluation and the collaboration in this field of activity.

Within the preparation for the European Data Protection Day several press releases were sent to the main Romanian news agencies (Rompres, Mediafax, News In), TV stations (Realitatea, including repeated mention on "crawl", National TV, TVr) and daily newspapers

(Cotidianul, Compact, Evenimentul Zilei). A press release on the significance of this event was also published on the Authority's web site.

Citizens were also informed on this European event via a publicity banner which read "28th January – the European Data Protection Day" posted throughout these events at the authority's premises and a similar one in the center of Tg. Jiu.

A brochure and a flyer were also issued on the occasion of this event. They were both titled "the European Data Protection Day" and were printed in Romanian and English. An additional brochure on "the protection of personal data and the right of access" was also issued in both languages. Other flyers and brochures such as 3"Know your rights" and "Personal Data" (the Authority's attributions) were updated.

all of this information material, together with promotional materials were spread amongst participants at the events on the European Data Protection Day, including media representatives.

Training youths on personal data protection also fits into the activities celebrating this event. This is why the Simion Bărnuțiu Law School in Sibiu included "data protection" on the list of its curricula for 2007/2008. Lectures have already been held by the Supervsory Authority's president. A particular interest was noticed amongst students with regard to this subject, fact which has also been indicated by the variety of subjects applied for examination during final exams. The members of the academic medium also played an important part throughout the school year as they have constantly requested form the Authority and spread mongst students information materials on personal data protection.

The Hyperion University in Bucharest has also shown its interest in including data protection as a subject of study. Contacts were made to include this field in the curricula of other universities as well.
The Increasing awareness with regard to the principles of personal data protection and the individual's right to private life have become a reality after the 28th January 2007, when the first celebration in honor of the European Data Protection Day were held.

*****

SLOVAK REPUBLIC

On the occasion of Data Protection Day on January 28th, the Office for Personal Data Protection of the Slovak Republic performed the following activities:

1. Imprinted the information markers with general information on the Office for Personal Data Protection of the Slovak Republic for the provision of contact information to general public and journalists as well.
2. Initiated set of broadcastings (together 5) in form of dialog with the President of the Office on topic "Personal data protection and risks of misuse" in a chosen radio channel. Inspector of the Office provided an interview for radio program "Our guest" and answered online the questions of listeners.
3. Participated in a discussion program of main Slovak Broadcast; the edition was dedicated specifically to this occasion; Office for Personal Data Protection of the Slovak Republic was represented by its president and the chief inspector
4. Introduced regular column in a printed media dedicated to the particular data protection issues and risks of the possible personal data misuse.
5. Refilled the office´s web page with a relevant content in regards to the general public´s expectation and needs, namely with "Statement of Vice-President Frattini on the occasion of the second Data Protection Day", "Be familiar with your rights" with information on Europol and rights of citizens, "Guidelines for controllers concerning international transfers of personal data".

6. Cooperated with Czech data protection authority and together with Slovak agency Neopublic will participate on common event dedicated to juveniles.
7. Participated on initiative called “Safely on Internet” with secondary title “Talk to your children about snares of Internet”. This initiative is aimed to protect children on Internet and within this initiative more than 500 teachers were trained in the mentioned field.

For this time, the general impression received by the media representatives was that they were not ready to assign for the entries of the president of the office, specifically on the 28.1.2008 the time and space needed, finding the issue for the general public not enough catching.

*****

SPAIN

Concerning to the 2nd Data Protection Day, these are the events organized by the Spanish DPA:

- We inserted advertisements on January the 27th on the main newspapers in Spain.
- Open day at the Spanish Data Protection Agency headquarters, with information about the data protection rights and principles. About 220 persons came to the Spanish DPA. It demonstrates the high interest and concerns of the society in their data protection rights.
- A significant group of students of one of the most important university in Spain came to visit the Spanish DPA and learn more about the data protection.
- The main press media published articles in radio, newspapers and TV.
- The Director of the Spanish DPA was interviewed in two TV News.
- Elaboration of a video on data protection rights that will be projected for the public at the Agency.

We have observed that the concerns of the citizens are more concrete than other years. There has been an increase of people from the last year. People who came demonstrated that they knew the basic principles of the data protection rights.

*****

“THE FORMAR YUGOSLAV REPUBLIC OF MACEDONIA”

On the occasion of the Data Protection Day, 28 January, the Directorate for personal data protection of the Republic of Macedonia (hereinafter: Directorate) organized set of activities whose primary aim was to raise awareness for personal data protection of the general public as well as of the controllers, both, in private and public sector.

Starting activity was the Press Conference on 27 January, 2008. The main topics on the Press Conference were:

Promotion of the brochure “It’s up to you”
Promotion of the video spot, part of the media campaign of the Directorate
Introducing the amendments of the Law on personal data protection
Central register - announcing the start of its putting into function

The Directorate welcomed the journalists and answered their questions and interests in personal data protection. Taking in consideration the interest of the journalists, we deem this activity as a successful one. Information about Data Protection Day and about Directorates’

experience was presented in most of the media (evening news (TV and Radio, newspapers)). Interest of the media for data protection was high during the whole week and Directorate had over 30 media appearances.

On 28 January 2008, Directorate organized Open day and realized it through two main activities:

Promotion of the brochure “It’s up to you”

Directorate invited three secondary schools to the promotion of the brochure. Three groups of 20 scholars attended the promotion. Promotion was organized as a debate and discussion with the scholars about protection of their personal data when using internet and in other every day situations.

Introducing the amendments of the Law on personal data protection and announcing the start of its putting into function Central register

28 January was Open day for the general public as well as for the controllers. The Directorates’ team prepared presentation for the key amendments of the Law on personal data protection and informed the citizens and controllers about the new possibilities and new obligations when data protection is considered.
On this day, the Central register was officially opened for all the controllers.

Taking in consideration the high interest of the citizens, controllers and journalists, we are happy to say that the celebration of the 28 January European data protection day was successful.