COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 14 November 2011

T-PD (2010) RAP 26 prov

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (ETS 108)

(T-PD)

26th plenary meeting
Strasbourg, 1-4 June 2010

DRAFT MEETING REPORT

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

I. OPENING OF THE MEETING 3
II. ADOPTION OF THE AGENDA 3
III. STATEMENT BY THE SECRETARIAT 3
IV. ELECTION OF THE T-PD CHAIR 3
V. MODIFICATIONS OF THE T-PD'S RULES OF PROCEDURE 4
VI. ELECTION OF THE TWO VICE-CHAIRS AND THE FOUR BUREAU MEMBERS OF THE T-PD 4
VII. UPDATES PROVIDED BY THE OBSERVERS TO THE COMMITTEE 5
VIII. PROFILING 5
IX. SUMMARY CONCERNING THE TERM OF OFFICE OF THE COUNCIL OF EUROPE DATA PROTECTION COMMISSIONER 9
X. ELECTION OF THE COUNCIL OF EUROPE DATA PROTECTION COMMISSIONER 9
XI. DRAFT REGULATION OUTLINING A DATA PROTECTION SYSTEM FOR PERSONAL DATA FILES IN THE COUNCIL OF EUROPE 9
XII. THE DATA PROTECTION DAY 2010 AND MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD 11
XIII. COMMUNICATION FROM THE SECRETARIAT OF THE STEERING COMMITTEE ON MEDIA AND NEW COMMUNICATION SERVICES 12
XIV. THE DATE OF THE NEXT PLENARY MEETING 12

I. OPENING OF THE MEETING

1. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), set up under Article 18 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), held its 26th meeting at the Council of Europe in Strasbourg from 1 to 4 June 2010.

2. The plenary session was opened by Mr Jörg Polakiewicz, Head of the Law Reform Department.

3. The list of participants is reproduced in Appendix I to this report.

II. ADOPTION OF THE AGENDA

4. The agenda as adopted by the T-PD is reproduced in Appendix II to this report, accompanied by a list of the documents relating to each of the items examined.

III. STATEMENT BY THE SECRETARIAT

5. Mr Jörg Polakiewicz welcomed the active contribution the T-PD had made to various European and international forums such as EuroDIG and the Internet Governance Forum. He noticed a growing interest in having international standards on data protection and the fight against cybercrime set up; the two subject matters also being priorities for the Secretary General of the Council of Europe. The contribution of the T-PD to the revision of the Convention on Mutual Administrative Assistance in Tax Matters (ETS No. 127) resulted in the drafting of the amending protocol opened for signature at the annual ministerial meeting of the OECD on 27-28 May 2010.

6. He reiterated that during this meeting the T-PD would vote on the draft recommendation on the protection of individuals with regard to automatic processing of data in the context of profiling. Never before had the call for international standards on profiling been so strong. Despite being a non-binding instrument, Council of Europe recommendations still had international authority.

7. The 30th anniversary of Convention No. 108, to be celebrated in 2011, would be an excellent opportunity to discuss the future of data protection.

IV. ELECTION OF THE T-PD CHAIR

8. The T-PD held the election of the Chair in accordance with Article 10 § 1 of the T-PD Rules of Procedure.

9. Mr Jean-Philippe Walter (Switzerland) was elected as Chair. He thanked the T-PD for its confidence. He said that the T-PD would face complex issues in the coming

years which would need to be dealt with, such as the revision of Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and Recommendation No. R (87) 15 regulating the use of personal data in the police sector. To this one should add a strong need to promote Convention No. 108 and its Additional Protocol among states which were not members of the Council of Europe. Achieving these objectives should be pursued in close cooperation with various stakeholders such as the European Commission, representatives of civil society, the International Chamber of Commerce and others. The T-PD's immediate objective was to finalise the draft recommendation on profiling.

V. MODIFICATIONS OF THE T-PD'S RULES OF PROCEDURE

10. The T-PD examined the amendments proposed by the T-PD Bureau at its meeting held in Lisbon on 13-15 April 2010. The amendment to Article 3 sought to clarify which internal Council of Europe bodies and institutions involved in the work on data protection were entitled to send their representatives to T-PD meetings. Furthermore, Article 3 stated that, if not decided otherwise, T-PD meetings were by default open to observers and experts referred to in Articles 3, 4 and 4a. The new wording of Article 9a confirmed an existing practice of adopting reports by the T-PD. The revised Article 10 was intended to clarify the procedure for election of the Chair and Vice-Presidents. Article 10a detailed the changes in composition, competences and working methods of the T-PD Bureau, which was the result of the reduction in the number of plenary meetings to one per year. Article 10b gave the Chair a casting vote in the event that an urgent vote on a text had to be taken by the Bureau. Article 13 provided for the possibility of holding the T-PD Bureau meeting in one official language only in the absence of technical facilities for simultaneous interpretation.
11. The T-PD adopted unanimously the T-PD's rules of procedure as amended (Appendix III) and decided to consider the amendments to Articles 14 and 15 at a later stage.

VI. ELECTION OF THE TWO VICE-CHAIRS AND THE FOUR BUREAU MEMBERS OF THE T-PD

12. Following a call for candidatures from the Secretariat prior to the meeting, eight applications were received from: Ms Georgeta Basarabescu (Romania), Ms Anne-Marije Fontein-Bijnsdorp (Netherlands), Ms Catherine Pozzo di Borgo (France), Mr Gérard Lommel (Luxembourg), Mr José Leandro Núñez García (Spain), Ms Alessandra Pierucci (Italy), Ms Hana Štěpánková (Czech Republic) and Mr David Törngren (Sweden).

13. Of these eight candidates, and in accordance with Rule 10 bis 2 of its Rules of Procedure, the T-PD elected Ms Hana Stepankova (Czech Republic) as the first Vice-Chair and Ms Catherine Pozzo-di-Borgo (France) as the second Vice-Chair.

14. Mr José Leandro Núñez García (Spain), Mr Gérard Lommel (Luxembourg), Ms Alessandra Pierucci (Italy) and Mr David Törngren (Sweden) were elected as the Bureau members for a term of office extending until 2012.

VII. UPDATES PROVIDED BY THE OBSERVERS TO THE COMMITTEE

15. The European Commission presented updates of its activity in the field of data protection. The 2009 conference organised by the Commission in the context of the revision of the EU data protection framework had received positive feedback from the private and public sectors. The Commission was working on amendments to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and was planning to present its legislative proposal by the end of 2010.

VIII. PROFILING

16. The T-PD considered the comments on the draft recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling (hereafter "the recommendation") submitted by the contracting parties, the observers and stakeholders.

The Preamble

17. Following some discussion the T-PD decided to amend recitals 2, 3 and 4 to stress different purposes for which profiling could be used.

18. The T-PD changed the wording of recital 5 accepting that the prediction of personal preferences, behaviour and attitudes were only non-exhaustive examples of profiling applications.

19. It was decided to emphasise in recital 6 the lack of knowledge that data subjects had about the use of profiling techniques.

20. It was noted that the reference to "services" in recital 11 should be interpreted widely so as to include the public sector alongside the commercial sector.

21. It was decided to remove the reference to the groups of people from recital 12 since the final purpose of the profiling would, in the end, always concern a given individual.

22. It was pointed out that the term "children" in recital 13 should be interpreted in the light of the Council of Europe's legal instruments. It was decided to specify the measures aimed at protecting children unable to give their consent to profiling.

Recommendations

23. It was stressed that the list of persons and bodies participating in and using profiling could not be exhaustive given the continuing advances in technology. Therefore,

paragraph 3 included non-exhaustive examples. Following some discussion, it was decided to replace the term “internet service providers” by a more general term “electronic communication service providers”.

Appendix to the recommendation

24. During the discussion on Principle 1 b, it was stressed that the list of sensitive data provided in Article 6 of Convention No. 108 should not be considered as exhaustive. More examples of “sensitive data” should be given in the explanatory memorandum.

25. It was suggested that further examples describing “profile” and “profiling” (Principles 1 d and 1 e) should be given in the explanatory memorandum.

26. It was noted that the wording used in Principle 1 f was similar to that in the e-commerce directive. Furthermore, the term “remuneration” referred to in this Principle also covered indirect remuneration; for example, remuneration through advertising. It was requested that further explanation be added to the explanatory memorandum.

27. With regard to the scope of the draft recommendation, it was reiterated that during the 25th plenary the T-PD had decided to limit the scope of the draft recommendation to the private sector. The T-PD Bureau had decided at a later stage to extend the scope of the text to include the public sector. This was justified by the difficulty which arose in drawing a clear line to distinguish between the two sectors; an example was given of private health and education entities which might receive contributions from public findings. Convention No. 108 did not differentiate between these two sectors either. It was reiterated that the decision taken at the 25th plenary session had aimed to exclude the so-called third pillar. However, after the Lisbon Treaty had come into force, pillar system considerations were not relevant anymore, which had led the T-PD Bureau to reconsider the scope of the draft recommendation. It was stressed that the police and judicial sectors had pecific needs; however, certain requirements, such as the principle of proportionality, should also be applicable to these areas. It was agreed, by a majority of votes cast, that the scope of the recommendation would not be limited as such but that member states would be given the possibility to foresee derogations by analogy to the approach adopted in Convention No. 108.

28. At the proposal of the representative of the European Commission, it was decided to add the principle of non-discrimination to Principles 2.1 and 2.2 given that this requirement was one of the most important in the Lisbon Treaty. The term “discrimination” ought to be detailed in the explanatory memorandum emphasising that differentiation and discrimination should not be confused. It was also decided to add to Principle 2.2 a reference to the principle of transparency while noting at the same time that profiling could not always grant full transparency. The term “arbitrary” in Principle 2.2 was replaced by the self-explanatory wording “contrary to the law”.

29. The T-PD decided to add to Chapter 2 a new Principle 2.3 which recommended states to take appropriate measures against the development and use of technologies which were aimed at the illicit circumvention of technical measures protecting privacy. It was stressed that the aim of this Principle was not to forbid these kinds of technologies as such but to guarantee their use for proper purposes. It encouraged a "privacy by design" approach to be detailed in the explanatory memorandum.

30. As regards Principle 3.4.a, it was stressed that the wording "if it is provided for by law" covered the legal obligation to collect and process data which may result in profiling. An example was given of a bank obliged to collect data concerning given money transfers using profiling as a means of enforcing this legal duty.

31. As regards Principle 3.4.b, it was decided to keep the wording "if it is permitted by law", which had been already used in other recommendations and meant that certain actions were not forbidden by law without being expressly authorised by it.

32. It was decided to move the provision about explicit consent for the processing of sensitive data from Principle 3.4.b first indent to Principle 3.11.

33. During the discussion on Principle 3.5 it was mentioned that people who could not express their free, specific and informed consent on their own behalf should not be generally profiled. Several T-PD members argued that this limitation was not in line with Directive 95/46/EC, which had adopted a more flexible approach. By a majority of votes cast it was decided to keep the wording as it stood in the draft.

34. It was proposed to clarify in Principle 3.7 that non-profiled access should be given to "information about goods and services" rather than "to goods and services" themselves. It was stressed that this provision expressed a concern that no cookies or other technologies of this kind should be stored by default and that an individual should not be pre-profiled while trying to get access to information on goods and services.

35. It was suggested that more explanation should be given regarding the data controller's duty of accuracy set out in Principle 3.9.

36. The T-PD discussed situations where data which had been collected for a given purpose without any intention for it to be used in profiling could nevertheless be processed in the context of profiling either for the initial or even a different purpose. It was stressed that the data controller had to have a proper legal basis for such subsequent processing, even if the initial collection of data had been lawful. The T-PD decided that this situation had to be explicitly mentioned in a separate provision and therefore added Principle 4.4.

37. The T-PD discussed the provision on informing data subjects of the possible effects and consequences of attributing profiles (Principle 4.1, last indent) and giving them information on the envisaged consequences of profiling (Principle 5.1.c). Some

members argued that the wording of Principle 4.1 last indent went beyond the requirements of Directive 95/46/EC by imposing additional duties on data controllers. Since data controllers were not able to foresee all possible effects and consequences of profiling, it was suggested speaking rather about “envisaged consequences”. The experts pointed out that it was crucial to inform data subjects of the effects and consequences of applying profiling which had a different meaning comparing to being informed about profiling purpose.. For example, the purpose of credit scoring was to evaluate credit worthiness, whereas its consequence would be the different costs of credit facilities or even the refusal to grant a loan. The representative of the European Commission reiterated that Directive 95/46/EC was deemed a directive of full harmonisation and any attempt to modify the scope of the obligations compared with those provided in the Directive might result in a distortion of the internal market. By a majority of votes cast it was decided to maintain Principle 4.1 last indent by replacing the words “possible effects and consequences” by “envisaged effects”. Regarding Principle 5.1.c, it was decided to add a condition “if not prohibited by law”.

38. At the proposal of the representative of the European Commission it was decided to modify Principle 5.1.b by adding the requirement to reveal the logic underpinning the processing of personal data “at least in the case of an automated decision”. However, since the aim of the provision was not to limit the right to have the logic revealed only in case of automated decisions, it was decided to emphasise in the explanatory memorandum the possibility available to states to go further in specifying the right of access to information concerning the logic underpinning the processing.

39. At the proposal of the representative of the European Commission it was decided to specify that data subjects’ rights should not adversely affect trade secrets or intellectual property. This limitation not being among those provided for in Convention No. 108, it was decided to mention it in the Preamble of the draft recommendation.

40. After the discussion underlining the difficulties in applying some of the principles of Chapters 3, 4 and 5 in the police and law-enforcement sectors, the T-PD decided to add a new chapter on exceptions available to member states. It was noted on this occasion that the general principles (Chapter 2) were not intended to create legal duties; therefore no exceptions should be applicable to Chapter 2.

41. It was noted that the expression “member states may foresee” in Principle 9.2 suggested that members states were given non-biding alternatives to foresee one of the proposed safeguards.

42. The T-PD adopted, with one abstention (the United Kingdom), the draft recommendation on profiling as amended.

43. The T-PD decided to send the draft recommendation to the European Committee on Legal Co-operation (CDCJ), which was invited to examine the text and to submit it to vote to the Committee of Ministers.

44. The Chair thanked the Secretariat, the T-PD members and observers and various stakeholders for their contribution to the work on the draft recommendation. T-PD members were invited to submit their comments and possible amendments to the draft explanatory memorandum to the draft recommendation.

IX. SUMMARY CONCERNING THE TERM OF OFFICE OF THE COUNCIL OF EUROPE DATA PROTECTION COMMISSIONER

45. The Council of Europe Data Protection Commissioner, Mr Karel Neuwirt, presented a summary concerning his three-year term of office. He regretted the lack of proper Commissioner's resources and the fact that internal regulations limited the Commissioner's competences. Under the current regulation outlining a data protection system for personal data files in the Council of Europe, the Commissioner is rather an honorary, position which makes setting up any activity difficult.

46. Mr Neuwirt noted that the Council of Europe staff regulations and other related documents were outdated and therefore needed to be redrafted. He emphasised a need for strengthening and defining the Commissioner's competences.

47. Mr Polakiewicz, on behalf of the Secretariat, stressed that the Council of Europe was committed to respecting data protection requirements. The Directorate of Internal Oversight, a new unit to be created, ought to be able to provide the Commissioner with the necessary resources.

X. ELECTION OF THE COUNCIL OF EUROPE DATA PROTECTION COMMISSIONER

48. Following a call for candidatures from the Chair, two applications for the office of Data Protection Commissioner were received from Mr Karel Neuwirt (Czech Republic) and Mr Clemence Misic (Slovenia).

49. The T-PD elected Mr Karel Neuwirt as the Council of Europe Data Protection Commissioner for a second term of office.

XI. DRAFT REGULATION OUTLINING A DATA PROTECTION SYSTEM FOR PERSONAL DATA FILES IN THE COUNCIL OF EUROPE

50. The T-PD discussed, in the presence of a representative of the Legal Advice Department, the revised draft Regulation outlining a data protection system for personal files in the Council of Europe prepared by the Data Protection Commissioner. It was noted that it was within the remit of the Data Protection Commissioner to present the revised draft Regulation to the Secretary General of

the Council of Europe. However, the T-PD decided to formulate some comments regarding the current draft.

51. The representative of the Legal Advice Department stressed that the current Regulation might be amended by a document issued by the Secretary General. However, there were some doubts regarding whether the Secretary General would be able to do so without approval from the Committee of Ministers given that the revised draft Regulation implied the transfer of some competences from the Secretary General to the Data Protection Commissioner.

52. It was underlined that the current rules for staff gave very limited access for third parties to the Council of Europe's administrative bodies and it was necessary to extend the Commissioner's competences with regard to access to documents and information.

53. It was proposed to mention the principle of access to official documents, which guaranteed the democratic functioning of institutions, in the preamble to the revised draft Regulation. It was also suggested that the possibility of making reference to the rules of court of the European Court of Human Rights be considered.

54. As regards Article 1 of the revised draft Regulation, it was recommended that personal data collected and processed by the Registry of the European Court of Human Rights and the Secretariat of the Parliamentary Assembly should also be covered by this Article. It was further suggested to have an explanatory note to the revised draft Regulation which would provide some explanations; for instance, to the definition of "personal data".

55. Concerning Article 2, it was noted that the term "lawfully" should be replaced by the term "in accordance with the applicable rules" to be in line with Council of Europe internal regulations.

56. As regards Article 3, the wording "any person shall be enabled to obtain" should be clarified in the explanatory note.

57. It was stressed that Article 5 paragraph 3 exclusively referred to the adoption of Council of Europe internal regulations aimed at defining the rights and obligations of data subjects when it came to personal data processing. The Commissioner was called to maintain dialogue with executive Council of Europe bodies in charge of adopting such internal regulations in order to be able to detect shortcomings at the adoption stage.

58. Regarding Article 6, it was suggested to give examples in the explanatory note of personal data transfer to third parties for legitimate purposes. For instance, such transfers could be undertaken for medical or insurance purposes in cases where a data subject was unable to give his or her prior consent. It was also stressed that even though the concept of an "adequate level of protection" referred to in Article 6 point f came from Convention No. 108, not all Council of Europe member states had

signed this Convention and, moreover, it was not embodied in the internal principles of the Council of Europe. Therefore, further explanation had to be given in the explanatory note. The same remark was made in respect of “sensitive data” referred to in Article 7.

59. It was pointed out that Article 8 paragraph 1 overlapped with Article 3 and therefore had to be deleted. It was also decided to delete Article 8 paragraph 2 which overlapped with Article 7 point a.

60. Concerning Article 4 of the Appendix, it was suggested that it should be explained in the explanatory note whether “confidential information” referred to in this Article was a third category of data, alongside personal data and sensitive data, or whether this was an umbrella term covering both of these categories.

61. It was noted that Article 5 of the Appendix should be more explicit. The wording “necessary infrastructure and resources” is too broad and could impose a significant financial burden on the Council of Europe. The meaning of this provision should be similar to that in other Council of Europe regulations, for example, in the mediators’ regulation.

62. It was stressed that the link between inquiries conducted by the Data Protection Commissioner under Article 7 of the Appendix and the procedure before the administrative tribunal of the Council of Europe should be clarified. It was suggested that the wording from other Council of Europe legal instruments be used, for example, from the document on the current procedure for combating harassment (Instruction No. 44 of the Secretary General).

63. In conclusion, the T-PD invited the Data Protection Commissioner to bring the revised draft regulation together with an explanatory note reflecting T-PD’s discussions to be prepared in cooperation with the T-PD Secretariat to the attention of the Secretary General of the Council of Europe.

XII. DATA PROTECTION DAY 2010 AND MAJOR DEVELOPMENTS IN THE FIELD OF DATA PROTECTION

64. The T-PD held a brief exchange of information on Data Protection Day 2010 as well as on recent national developments in the field of data protection.

65. The T-PD heard the report by Mr José Leandro Núñez García (Spain) on the cooperation with the World Anti-Doping Agency (WADA) and by Ms Rita Vaitkevičienė (Lithuania) on the recent work of the Steering Committee on Bioethics regarding Predictivity, Genetic Tests and Insurance.

66. The T-PD also invited all delegations to send the relevant information on national developments so it could be included in the appendix to this report (Appendix IV).

XIII. COMMUNICATION FROM THE SECRETARIAT OF THE STEERING COMMITTEE ON MEDIA AND NEW COMMUNICATION SERVICES

67. Mr Lee Hibbard, representative of the Media and Information Society Division, provided information on the third edition of the EuroDIG meeting that took place in Madrid and informed the participants of the next EuroDIG meeting to be held in Belgrade in June 2011 and the next Internet Governance Forum to be held in Vilnius in September 2010, which would be addressing the issues of cloud computing, security and privacy policies, social networks and intermediary liability. The importance of multi-stakeholders dialogue was stressed, especially within the international internet forums.

XIV. THE DATE OF THE NEXT PLENARY MEETING

68. The T-PD took note of the date of the next plenary meeting, to be held in Strasbourg from 29 November to 2 December 2010.

APPENDIX I

LIST OF PARTICIPANTS / *LISTE DES PARTICIPANTS*

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

ALBANIE/ALBANIA

Flora Çabej Pogaçe, Albanian Commissioner for Personal Data Protection, Rruga Abdi Toptani, Ish godina e Ministrise te Transporteve dhe Telekomunikacionit, Kati i dyte, Tirana

Erton Karagjozi, Director of the Registration Department, Commissioner for Personal Data Protection, Rr "Abdi Toptani, Nr. 4, Kati i II-te, Tirana, Albania

ANDORRA/ANDORRE

Florencia Aleix, Représentante permanente adjointe de l'Andorre auprès du Conseil de l'Europe, 10 avenue du Président Robert Schuman, 67000 Strasbourg

AUSTRIA/AUTRICHE

Eva Souhrada-Kirchmayer, *[First Vice-Chair of the T-PD],* Head of the data protection division, Federal Chancellery, Division V/3, Ballhausplatz 2, A-1014 Vienna

BELGIUM/BELGIQUE

Joëlle Jouret, SPF Justice, Direction générale de la législation et des libertés et droits fondamentaux, Service des droits de l'homme, Cellule vie privée, 115 boulevard de Waterloo, 1000 Bruxelles

BOSNIA AND HERZEGOVINA / BOSNIE HERZEGOVINE

Samira Campara, Director Assistant, Agency for personal data protection, Street Vilsonovo setaliste 10, 71000 Sarajevo

Selma Maksumic, Assistant, Agency for personal data protection, Street Vilsonovo setaliste 10 71000 Sarajevo

CROATIA/CROATIE

Vilena Gašparović, Deputy Director, Croatian Personal Data Protection Agency, Republike Austrije 25, 10000 Zagreb
Tel.: +385 (0)1 46 090 14
vilena.gasparovic@azop.hr

Lana Velimirović Vukalović, M.A., Advisor at the Director's Office and Spokesperson, Croatian Personal Data Protection Agency, Republike Austrije 25, 10000 Zagreb

CYPRUS/CHYPRE

Nonie Avraam, Office of the Commissioner for personal data protection, 1 Iasonos Str, 1082 Nicosia

CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE

Hana Štěpánková, Head of the Press Department, Spokeswoman, Office for Personal Data Protection, Pplk.Sochora 27, 170 00 Prague 7

DENMARK/DANEMARK

Astrid Gade, Head of Section, Datatilsynet, Borgergade 28, 5, 1300 København K

ESTONIA/ESTONIE

Kaja Puusepp, Supervision Director, Estonian Data Protection Inspectorate, Väike-Amerika 19 -10129 Tallinn

FINLAND/FINLANDE

Leena Rantalankila, Ministerial Adviser, Ministry of Justice, PO Box 25, FIN-00023 Gov.

FRANCE

Mme Catherine Pozzo di Borgo, Commissaire du Gouvernement adjoint auprès de la CNIL, Services du Premier Ministre, 66 rue de Bellechasse 75007 Paris

GERMANY/ALLEMAGNE

Stefan Sobotta, Ministry of the Interior, Division V II 4 Data Protection Law, 11014 Berlin

GEORGIA/GEORGIE

Giorgi Jokhadze, Head of Analytical Department, Ministry of Justice, 24 Gorgasali Str., 0133 Tbilisi,

HUNGARY/HONGRIE

Kinga Szurday, Senior legal councellor, Ministry of Justice and law enforcement, Kossuth ter 4, Budapest 1055
Tel.: +36 1 441 3935 ; Fax +36 1 441 2932
szurdayk@irm.gov.hu

IRELAND/IRLANDE

Ms Noreen Walsh, Civil Law Reform Division, Department of Justice, Equality and Law Reform, Bishop's Square, Redmond's Hill, Dublin 2

ITALY/ITALIE

Alessandra Pierucci, Civil Servant at the Italian Data Protection Authority, Garante per la Protezione dei Dati Personali, Piazza di Monte Citorio 121, 00186 Rome

LATVIA/LETTONIE

Signe Plumina, Director, Data State Inspectorate of Latvia, Blaumana Str 11/13-15, LV-1011 Riga

Aiga Balode, Deputy Director, Data State Inspectorate of Latvia, Blaumana Str 11/13-15, LV-1011 Riga

LITHUANIA/LITUANIE

Rita Vaitkevičienė, Deputy Director, State Data Protection Inspectorate, A. Juozapavičiaus str. 6 , Slucko str. 2, 09310 Vilnius

LIECHSTENSTEIN

Philipp Mittelberger, Datenschutzbeauftragter, Stabsstelle für Datenschutz (Data Protection Office), Haus Wille, Kirchstrasse 8, 9490 Vaduz

LUXEMBOURG

Gérard Lommel, Président de la Commission Nationale pour la protection des données, 41 rue de la Gare, 1611 Luxembourg

MALTA/MALTE

Ingrid Camilleri B.A., Head of Legal Unit, Office of the Data Protection Commissioner, 2 Airwars House, High Street Sliema SLM 16

MOLDOVA

Valentina Popovici, Deputy Director of the Scientific Research and Analysis Division of the Ministry of Informational Technologies, Stefan cel Mare str. 134, MD-2012 Chisinau

NETHERLANDS/PAYS-BAS

Excused/excusé

NORWAY/NORVEGE

Birgitte Istad, Adviser, Ministry of Justice, PO Box 8005 Dep., 0030 Oslo

POLAND/POLOGNE

Urszula Góral, Director, Social Education and International Cooperation Department, Bureau of the Inspector General for Personal Data Protection, ul. Stawki 2, 00-193 Warszawa

PORTUGAL

Joao Pedro Cabral, *[Chair of the T-PD],* Directorate General of Justice Policy, Ministry of Justice, Avenida Óscar Monteiro Torres, n.º 39, 1000-216 Lisboa

Cláudia Maduro Redinha , Directorate General of Justice Policy, Ministry of Justice, Avenida Óscar Monteiro Torres, n.º 39, 1000-216 Lisboa

ROMANIA/ROUMANIE

Ms Georgeta Basarabescu, President of the National Supervisory Authority for Personal Data Processing, Olari street no. 32 2nd district, Bucharest 024057

George Grigore, Department of European Integration, and International Affairs - Romanian DPA - Olari street no. 32, 2nd district, 024057 Bucharest

SERBIA/SERBIE

Nevena Ruzic, Commissioner for Information of Public Importance and Personal Data Protection, Head of the Office, 42 Svetozara Markovica, 11000 Belgrade

SLOVAKIA/SLOVAQUIE

Veronika Žuffová–Kunčová, State Counselor, Foreign Relations Department, Personal Data Protection Office of the SR, Odborárske námestie 3, 817 60 Bratislava 15

SLOVENIA/SLOVENIE

Marijan Conc, State Supervisor for personal data , Information Commissioner Office, Vosnjakova 1, p.p. 78, 1001 Ljubljana

SPAIN/ESPAGNE

José Leandro Núñez García, Legal Advisor, International Section of the Spanish Data Protection Agency, Agencia Española de Protección de Datos, C/Jorge Juan 6, 28001 Madrid

SWEDEN/SUEDE

Eva Lenberg, Director, Ministry of Justice, 10333 Stockholm

David Törngren, Legal Adviser, Ministry of Justice, 10333 Stockholm

SWITZERLAND/SUISSE

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, Feldeggweg 1, 3003 Berne

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

Marijana Marusic, Director, Directorate for Personal Data Protection, Street Samoilova 10, 1000 Skopje

UNITED KINGDOM/ROYAUME-UNI

Kevin Fraser, Head of EU Data Protection Policy, Ministry of Justice, 102 Petty France, London SW1H 9AJ

EXPERTS SCIENTIFIQUES/SCIENTIFIC EXPERTS

Yves Poullet, Directeur du CRID (Centre de Recherches Informatique et Droit, Faculté de Droit, 5 Rempart de la Vierge, 5000 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, 61 rue de Bruxelles, 5000 Namur, Belgique

COMMISSION OF THE EUROPEAN COMMUNITIES/

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Hana Pecháčková, Directorate General Justice, Freedom and Security, D5 Data Protection Unit, Office LX 46 01/14, 46 rue du Luxembourg, 1000 Brussels

Sven Röhr, DG Health and Consumers F101 06/047, Unit B2, Consumer Contract and Marketing Law, B – 1049 Brussels

OBSERVERS/OBSERVATEURS

MEXICO / MEXIQUE

María Marván Laborde**,** Commissioner of the Federal Institute of Access to Public Information (IFAI) of Mexico, Av. México # 151, Col. El Carmen, Coyoacán, C.P. 04100, Delegación Coyoacán, México D.F.

FRENCH-SPEAKING ASSOCIATION OF PERSONAL DATA PROTECTION AUTHORITIES / ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES (AFAPDP)

Olivier Matter, CNIL, Secrétariat Général de l'AFAPDP, 8 rue Vivienne, CS 30223, 75083 Paris Cedex 08

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

Christopher Kuner, Hunton & Williams, Park Atrium, rue des Colonies 11, B-1000 Brussels

INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS / CONFERENCE INTERNATIONALE DES COMMISSAIRES A LA PROTECTION DES DONNEES ET DE LA VIE PRIVEE

Alessandra Pierucci, Garante per la Protezione dei Dati Personali, Piazza di Monte Citorio 121, 00186 Rome

IBERO-AMERICAN DATA PROTECTION NETWORK / RESEAU IBERO-AMERICAIN DE PROTECTION DES DONNEES

María Marván Laborde**,** Commissioner of the Federal Institute of Access to Public Information (IFAI) of Mexico, Av. México # 151, Col. El Carmen, Coyoacán, C.P. 04100, Delegación Coyoacán, México D.F.

INVITED/INVITES

EUROPEAN PRIVACY ASSOCIATION

Karin Riis-Jorgensen, Chairwoman and Funder of the European Privacy Association, Franklinstraat 106-108, 1000 Brussels, Belgium

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

Law reform Department / Département des Réformes législatives

Jörg Polakiewicz, Head of the Law Reform Department / Chef du Service des réformes législatives ;

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

Data Protection / Protection des données :

Kateryna Gayevska, Secretary of the TPD / Secrétaire du T-PD

Lucy Ancelin, Assistant / Assistante

Claire Genevay, Trainee / Stagiaire

Christiane Weltzer, Assistant / Assistante,

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**

Lee Hibbard, Administrator / Administrateur

Franziska Klopfer, Administrator / Administrateur

DIRECTORATE GENERAL III – SOCIAL COHESION / DIRECTION GENERALE III – COHESION SOCIALE

Bioethics Division / Division de la Bioethique

Laurence Lwoff, Head of Division/Chef de la Division

Aysegül Elveris, Administrator/Administrateur

DIRECTORATE GENERAL OF EDUCATION, CULTURE AND HERITAGE, YOUTH AND SPORT, DIRECTION GENERALE DE L'EDUCATION, DE LA CULTURE ET DU PATRIMOINE, DE LA JEUNESSE ET DU SPORT

Sport Department / Service du sport

Markus Adelsbach, Head of Sport Conventions / Chef de la division des Conventions du sport

INTERPRETERS/INTERPRETES

Cynera JAFFREY
Nicolas GUITTONNEAU
Christine TRAPP-GILL

APPENDIX II

DRAFT AGENDA

OPENING OF THE MEETING

ADOPTION OF THE AGENDA

STATEMENT BY THE SECRETARIAT

• T-PD (2008) RAP 25	Report of the 25th Plenary meeting of the T-PD (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108]) (2-4 September 2009)
• CM/Del/Dec(2010)1079/10.2	Committee of Minister's decision on Draft Abridged report of the 25th Plenary meeting of the T-PD
• T-PD-BUR (2009) RAP 19	Report of the 19th meeting of the T-PD-BUR (18-20 November 2009)
• T-PD-BUR (2010) RAP 20	Report of the 20th meeting of the T-PD-BUR (2-4 March 2010)
• T-PD-BUR (2010) RAP 21	Report of the 21th meeting of the T-PD-BUR (13-15 April 2010)

ELECTION OF THE CHAIR, VICE-CHAIRS AND THE BUREAU MEMBERS

Required action: the T-PD will elect its Chair, two Vice-chairs and the Bureau members

OVERVIEW OF DATA PROTECTION ACTIVITIES SINCE THE LAST PLENARY AND PARTICIPATION OF T-PD MEMBERS AT OTHER WORKING GROUPS (CAHTAX, ANTI-DOPING ETC)

Required action: the T-PD members will take note of the participation of the T-PD members at other working parties.

UPDATES FROM OBSERVERS

PROFILING

Required action: the T-PD will be called upon to examine the draft recommendation on personal data protection with regards to the process of profiling with a view to its adoption

• T-PD (2008) 1	Final version of the study on the application of

Convention 108 to the profiling mechanisms

- T-PD-BUR(2009)2Rev5 Fin — Draft recommendation on the protection of individuals with regard to automatic processing of personal data used in the framework of profiling as resulting from the 21th Bureau meeting (13-15 April 2010)
- T-PD-BUR (2010) 05 — Comments on the 5th version of the draft recommendation on the protection of individuals with regard to automatic processing of personal data used in the framework of profiling
- T-PD-BUR (2010) 02 — Explanatory memorandum on the draft recommendation on the protection of individuals with regard to automatic processing of personal data used in the framework of profiling

ELECTION OF THE DATA PROTECTION COMMISSIONER

Required action: According to Article 1 of the Resolution on the Regulation outlining a data protection system for personal data files in the Council of Europe, the T-PD will elect the Data Protection Commissioner of the Council of Europe..

DISCUSSION ON A NEW RESOLUTION ON DATA PROTECTION COMMISSIONER

Required action: the T-PD will discuss the amendments proposed to the resolution on the Regulation outlining a data protection system for personal data files in the Council of Europe with a view to sending it to the Secretary General of the Council of Europe

T-PD-BUR (2010) 06 — Draft Regulation outlining a data protection system for personal data files in the Council of Europe

AMENDMENTS TO THE RULES OF PROCEDURE

Required action: the T-PD will be called upon to discuss the proposed amendments to the rules of procedure with a view to its adoption

- T-PD (2010) 01 — Draft rules of procedure

DATA INFORMATION ON THE 2010 DATA PROTECTION DAY AND ON MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD SINCE THE 25TH MEETING OF THE T-PD (2-4 SEPEMBER 2010)

Required action: the T-PD will have an exchange of views on those issues. Delegations are encouraged to submit their contributions in writing to the Secretariat by the 15th of May

- DPD (2010) Compilation — Compilation of the participation forms received for the 2010 Data Protection Day
- T-PD (2010) 02 — Information on recent developments at national level in the data protection field

DATE OF THE 27TH PLENARY MEETING OF THE T-PD IN 2011

APPENDIX III

Strasbourg, 19 May 2010 T-PD(2010) 01 prov

CONSULTATIVE COMMITTEE OF THE CONVENTION

FOR THE PROTECTION OF INDIVIDUALS

WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD)

26th plenary meeting
1-4 June 2010
Strasbourg, Agora Building, Room G02

MODIFICATION OF THE T-PD's RULES OF PROCEDURE

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

Rules of procedure of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108).

The Consultative Committee,

Having regard to the entry into force on 1 October 1985 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,

Having regard to Article 20, paragraph 4 of the Convention,

Adopts the present Rules of Procedure:

Article 1:

For the purposes of the Rules of Procedure, the following definitions are used:

- "Convention", means the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data;

- "Committee", means the Consultative Committee of the Convention;

- "Representative", means the representative of a Contracting Party or, in his absence, the deputy representative appointed in accordance with the provisions of Article 18, paragraph 2 of the Convention;

- "Observer", means the observer of a member State of the Council of Europe which has not yet become a Party to the Convention as well as the observer of a non-member State appointed in accordance with the provisions of Article 18 paragraph 3 of the Convention.

- “Written procedure” means a distance voting process, using for instance electronic mail, telecopy or postal mail. [V]

Article 2: Representatives

1. Each Contracting Party shall communicate to the Secretary General of the Council of Europe, the name, address and functions of its representative to the Committee, of his deputy and, if necessary, of his advisers.

2. Each representative shall retain office until the Contracting Party has notified the Secretary General that the representative has been replaced.

Article 3: Observers

1. Any member State of the Council of Europe which is not a Party to the Convention shall communicate to the Secretary General of the Council of Europe the name, address and functions of the person appointed as its observer and, if necessary, of his adviser. The person appointed as observer shall retain office until the member State has notified the Secretary General of the Council of Europe that he has been replaced.

2. Any non-member State of the Council of Europe which is not a Party to the Convention shall communicate the name, address and functions of the person appointed as its observer, in accordance with the conditions laid down in Article 18, paragraph 3 of the Convention.

3. Abstentions which may be accompanied by an explanatory statement shall not prevent the Committee from reaching a decision in accordance with Article 18, paragraph 3 of the Convention.

4. The following Council of Europe bodies may send a representative to meetings of the Committee, without the right to vote but with defrayal of expenses at the charge of their respective Votes of the Ordinary Budget:

- the Parliamentary Assembly,

- the Congress of Local and Regional Authorities of the Council of Europe,

- the European Court of Human Rights,

- the Commissioner for Human Rights,

- the Conference of INGOs enjoying participatory status with the Council of Europe,

- the Steering Committee for Human Rights (CDDH);

- the European Committee on Legal Co-operation (CDCJ),

- the European Committee on Crime Problems (CDPC),

- the Steering Committee on the Media and New Communication Services (CDMC).

5. The Data Protection Commissioner of the Council of Europe may also participate in the meetings of the Committee, without the right to vote but with defrayal of his or her expenses.

6. The Committee or its Bureau may decide to hold a whole meeting or a part of the meeting without the presence of observers referred to in Articles 2 and 3 of the current rules of procedure.

Alternative wording:
6. Meetings are by default open to observers referred to in Articles 3 and 4 unless stated otherwise.

Article 4: Experts

1. The Committee may, by unanimity of the votes cast, decide to invite a person, or invite an Organisation to appoint a person, to participate in the work of the Committee as an expert or who may be available for consultation during all or part of a meeting.

2. The Organisation concerned shall communicate to the Secretary General of the Council of Europe, the name, address and functions of the person appointed.

Article 4 bis: International Institutions and Organisations

1. The Committee may, by unanimity of the votes cast, decide to invite international Institutions and Organisations to send one or more delegates to attend its meetings.

2. Abstentions which may be accompanied by an explanatory statement shall not prevent the Committee from reaching a decision in accordance with Article 18, paragraph 3 of the Convention.

3. The Committee may, by a majority of the votes cast, decide to withdraw such an invitation. **(I)**

Article 5: Time limits for Notifications

The appointments referred to in Articles 2, 3 and 4 should as far as possible be notified at least one month before the date fixed for the opening of the meeting at which the persons appointed are to participate.

Article 6: Meetings

1. The Committee shall fix the dates of its meetings in consultation with the Secretary General.

2. The period between two meetings shall not exceed two years.

3. If one third of the representatives requests the convocation of the Committee, the Secretary General shall fix the date of the meeting in consultation with the Chairman of the Committee. This meeting shall take place, at the latest, four months after receipt of the request.

4. As a general rule, meetings shall be held at the seat of the Council of Europe in Strasbourg or at the Paris Office of the Council of Europe.

Article 7: Convocation

1. The meetings of the Committee shall be convened by letter of the Secretary General sent to the Governments, representatives and observers as well as to the experts invited in accordance with Article 4 of the Rules of Procedure.

2. The letter of convocation, accompanied by the draft agenda, shall be sent at least six weeks before the date fixed for the opening of the meeting. **(V)**

Article 8: Meeting Adjournment

After a meeting has been convened, any request for adjournment must be sent to the Secretary General at least two weeks before the original date fixed for the opening of the meeting. The request for adjournment will be considered as approved when the majority of representatives have made known their approval to the Secretary General seven days before the date originally fixed.

Article 9: Quorum

A majority of the representatives shall constitute a quorum for a meeting of the Committee.

Article 9 bis: **Functions and competences**

The Committee shall exercise the functions set out in Articles 19 and 20 of Convention. In particular, the Committee;

1. shall adopt the work programme and determine priorities;

2. shall draw up draft legal instruments [1] with a view to their adoption by the Committee of Ministers;

3. shall adopt opinions and reports;

[1] Namely conventions or agreements and recommendations.

4. shall decide on the establishment of working parties, on their composition and on their terms of reference

5. shall elect a chair and two vice-chairs and the other members of the Bureau following the requirements set out in Articles 10 bis and 10 ter;

6. shall adopt the terms of reference of the Bureau.[IV]

Article 10: Chair and Vice-Chairs

1. The Chair, the first Vice-Chair and the second Vice-Chair shall be elected by a majority of the members present from among the representatives for a period of two years. The elections shall not, by default, be held by secret ballot unless specifically requested.

2. The Chair and a Vice-Chair shall be eligible for re-election for a second consecutive term of office. However, their term of the Office Chair shall end if he or she ceases to be a member of the Committee.

3. The Chair shall direct the work and sum up the conclusions of the discussions.

4. The Chair shall retain the right to participate in the discussions of the Committee and to vote.

5. Whenever the Chair is absent or stands down, he shall be replaced in his role as Chair by the first Vice-Chair or if he or she is not available, the second Vice-Chair. If neither the Chair nor one or the other of the Vice-Chair can carry out his or her duties the Committee shall elect an acting Chair.

Article 10 bis: Membership, functions and competences of the Bureau

1. The Bureau shall be composed of the Chair and two Vice-chairs of the Committee, together with four elected members and the outgoing Chair who may remain a member *de iure* of the Bureau during the mandate(s) of the new Chair. The other members shall be elected from among the representatives on the Committee for a period of two years. The members shall be eligible for re-election.

2. If a member of the Bureau ceases to be a member of the Committee or resigns his/her office before its normal expiry, the Committee may elect a successor for the remainder of the term of that office.

3. The Bureau shall direct the work of the Committee between plenary meetings, and in particular:

a. prepare preliminary draft legal instruments and draft opinions provided for in Article 19 d of the Convention; [II]

b. prepare and approve opinions requested by Council of Europe bodies;

c. prepare reports taking into account of the comments of the Committee delegations, where possible, unless the report is urgent;

d. prepare the programme of activities and propose priorities to the Committee for future work according to the Committee' working programme with a suggested timetable;

e. review the agenda of the plenary meeting and propose the way the Committee's business should be dealt with (for example, drafting the order of business, indentifying issues of particular importance, etc)

f. invite external guest speakers, where appropriate;

g. appoint experts to carry out specific activities;

h. make appointments to other Council of Europe bodies;

i. to report back to the Committee on its activities between the plenary meetings; preparing;

j. deal with any other matters specifically delegated to it by the Committee.

4. Before taking a decision and without prejudice to Article 10 bis , paragraph 2 (c) and (j), the Bureau shall consult the members of the Committee and take their observations into account.. When the Bureau exercises the powers of the Committee, its decisions shall be taken by consensus. Where there is disagreement, it shall submit its draft decision to the Committee. **(IV)**

Article 10 ter: **Procedure** (VI)

1. The texts within the meaning of Article 9 bis paragraphs 5 and 6, submitted for the approval of the Committee shall be prepared by the Bureau. As a general rule they shall be subject to two readings by the Committee. A text may exceptionally be subject to a third reading if two-thirds of the representatives present at the second reading so request. During the second and third readings only those amendments presented in writing at least one month before the plenary meeting shall be debated.

2. As a general rule the Bureau shall adopt the texts it submits to the Committee by consensus. Where there is disagreement, the texts shall be adopted by a simple majority. The minority may present its point of view to the Committee in writing if it informs the Bureau beforehand. Once a text has been adopted, it shall be presented to the Committee by a rapporteur appointed by the Bureau. [In urgent cases, the Chair shall have the deciding vote.]

3. All proposals by the Bureau shall be sent to the members of the committee, who shall have four weeks in which to send their observations to the Secretariat who shall forward them to all members of the Committee. . This time limit may be reduced to two weeks in urgent cases. (VII)

4. Where documents are sent by electronic mail, the Secretariat shall take the necessary measures to ensure that the electronic mail messages have reached the members of the Committee. (IV)

Article 11: Secretariat

1. The Secretary General shall provide the Committee with the necessary staff and facilities.

2. The Secretary General or his representative may at any time make an oral or written statement on any matter under discussion or other relevant matters.

3. The Secretariat shall be responsible for the preparation and distribution of all documents to be examined by the Committee.

4. The Committee may ask the Secretariat to draw up a report, a document or a study on any question within the framework of the work of the Committee and if necessary with the assistance of experts.

5. The Secretary General shall ensure that the Committee is informed of the activities of other Committees or organs of the Council of Europe which may have a bearing on the discharge of its functions.

Article 12: Agenda

1. The Agenda shall be adopted at the beginning of each meeting on the basis of a draft prepared by the Secretariat in consultation with the Chair of the Committee.

2. All proposals for inclusion on the agenda shall be communicated at least one month before the date fixed for the meeting to the Secretariat, who shall send them to the addressees of the letter of convocation.

3. Any document submitted in a language other than one of the official languages shall be accompanied by a translation into one of the official languages.

Article 13: Languages

1. The official and working languages of the Committee shall be English and French. The Bureau may decide by unanimity to hold a particular meeting in only one of those languages.

2. Any representative or observer may, however, use a language other than an official language provided that he or she shall himself or herself provide for interpretation into one of the official languages.

Article 14: Publicity

1. Meetings shall be held in private. The Committee may decide to make public certain of its documents.

2. The Committee may, by unanimous agreement decide, at the end of its meeting, to make appropriate press statements on the decisions taken during the meeting.

Article 15: Voting

1. Subject to the provisions of Article 18 paragraph 3 of the Convention and of Article 4, Article 4 bis (I) and Article 14 paragraph 2, of the Rules of Procedure, the Committee shall take its decisions by a majority of the votes cast.

2. However, in matters falling within the competence of the European Union, when requested by a majority of the representatives of the Parties present, including a majority of the representatives of non-member States of the European Union, the Consultative Committee shall take a decision by a unanimous vote. (III)

Comment : The Bureau considered the possibility that within the meaning of articles 15 and 16 the decision to reconsider a vote should no longer take into account the criteria of being or not a member of the EU.

3. Decisions may be submitted to a vote by written procedure if decided unanimously by the Committee. In urgent cases, a question may be submitted to a decision by written procedure at the initiative of the Chair and the agreement of the vice-chairs. (V)

4. The draft decision which is subject to a written procedure shall be sent by the Secretariat to the representatives. The representatives shall expressly acknowledge receipt of the draft. The representatives shall inform the Secretariat of their vote in writing within a fixed term and in no case in less than 4 weeks, except in urgent cases. In urgent cases, the fixed term is decided by the Chair with the agreement of the Vice-Chairs and may not be

less than two weeks. Failure to inform the Secretariat in such term shall be considered to be an abstention. The Secretariat shall inform the representatives of the results of the vote. The result of the vote is recorded in the report of the following meeting of the Committee. (V)

5. The written procedure initiated by the Chair shall be interrupted if one representative requests within 7 days of receiving the draft that the draft be discussed during a meeting of the Committee, unless a majority of the representatives requests that the procedure goes ahead. (V)

Article 16: Reconsideration of a decision

When a decision has been taken on any particular matter, such matter shall not be reopened except at the request of a representative and with the approval of a majority of the votes cast. In matters falling within the competence of the European Union, a decision shall also be reconsidered if at least two thirds of all Parties to the Convention which are not members of the European Union so request. **(III)**

Article 17: Decisions and reports

The Secretariat shall prepare an abridged meeting report before the end of each meeting which will serve as a basis for the report provided for in Article 20, paragraph 3 of the Convention.

Article 18: Requests for opinion under Article 19 (d) of the Convention

1. Any request for an opinion addressed to the Committee by virtue of Article 19 (d) of the Convention, shall be made in writing.

2. The request shall be communicated by the Secretariat to the representatives and to the observers.

3. The request shall be included in the draft agenda of the first meeting to be held after receipt of the request.

4. If the Committee does not express an unanimous opinion, mention shall be made in the report of the minority opinions if the authors so request.

5. The text of the opinion shall be communicated to the Governments of the Contracting Parties and to the observers.

Article 19: Proposals made under Article 19 (a) of the Convention

Any proposal aimed at facilitating or improving the application of the Convention shall be communicated to the Committee of Ministers as well as to the Governments of the Contracting Parties and to the observers.

VIII. The rules of procedure were amended by the Consultative Committee at the 25th plenary meeting

VII. Paragraph amended by the T-PD in July 2008 after written procedure.

VI. Article 10 ter amended by the Consultative Committee further to its 24th meeting (13-14 March 2008)

V. Text inserted or amended by the Consultative Committee at its 24th meeting (13-14 March 2008)

IV. Article 9 bis, Article 10 bis, Article 10 ter were inserted by the consultative Committee at its 19th meeting (26-28 November 2003)

III. Text amended by the Consultative Committee at its 14th meeting (3 September 1998).

II. Amended by the Consultative Committee at its 19th meeting (26-28 November 2003)

I. Article 4 bis was inserted and the text was amended by the Consultative Committee at its 6th meeting (February 1992).

APPENDIX IV

Strasbourg, 21 May / mai 2010

T-PD (2010) 2
version mosaic / mosaïque
restricted

CONSULTATIVE COMMITTEE OF THE CONVENTION

FOR THE PROTECTION OF INDIVIDUALS

WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

/

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION

DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE

DES DONNEES A CARACTERE PERSONNEL

(T-PD)

1-4 June / juin 2010
26th plenary meeting / 26ème *réunion plénière*, Strasbourg
"Agora", room / *salle* G02

INFORMATION ON RECENT DEVELOPMENTS AT NATIONAL LEVEL IN THE DATA PROTECTION FIELD

/

COMMUNICATIONS SUR LES DÉVELOPPEMENTS RÉCENTS INTERVENUS DANS LE DOMAINE DE LA PROTECTION DES DONNÉES AU NIVEAU NATIONAL

Secretariat document prepared by
the Directorate General of Human Rights and Legal Affairs
Document du Secrétariat préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

TABLE / TABLE DES MATIERES

ALBANIA 32
CROATIA 37
CYPRUS 40
Czech republic 41
ESTONIA 43
FINLAND 44
ITALY 47
LATVIA 55
LITHUANIA 59
MACEDONIA 69
MALTA 79
NETHERLANDS 80
POLAND 85
PORTUGAL 89
SLOVAKIA 90
SLOVENIA 94
SPAIN 100

ALBANIA

Progress Report of the Albanian Commissioner's Office for Personal Data Protection

1. Stucture of the Commissioner's Office

The majority of the workforce was hired from July 2009 and by January 2010 the Office has filled all 29 positions it was allocated by the Assembly, as the internal structure and organization of the Office was approved by the decision of the Assembly no.225, dated 13.9.2008.

In its structure the Commissioner's Office comprises the Commissioner, the Adviser, the Secretary and 5 Department: Legal Procedural Affairs and Foreign Relations Department (Director and 5 Legal Experts), Registration Department (Director and 4 Experts), Inspection Department (Director and 4 Legal Experts (Inspectors), Public Relations Department (Director, 1 Expert and 2 IT Experts) and Supporting Services Department (HR) (Director and 6 Staff Members).

2. Legal Approach

2.1 Approved Decisions of the Council of Ministers

For the implementation of the law for the Personal Data Protection and the functioning effectively of the Institution, are drafted by the Commissioner's Office and approved by the Council of Ministers the Decisions:

- No. 934, dated 2.09.2009 "For the determination of the States with adequate level of the data protection". Drafting this decision was an obligation of article 8, Law nr. 9887, dated 10.03.2008 on the "Personal Data Protection".

- No. 1232 dated 11.12.2009 "On defining the cases for exemptions from the duty to notify the personal data processed", as the obligation set forth in Article 21, point 4 of the law.

2.2 Drafting and approval of Commissioner's Acts:

- Commissioner's office Internal regulation, which sets rules for organizing and functioning of the Office, as well as the competences, rights and obligations of the employees of the Commissioner's Office, approved by the Commissioner's Order No. 48, dated 31.07.2009;

- Commissioner's office Code of Ethics, which foresees rules on conduct of the employee of the Commissioner's Office, approved by the Commissioner's Order No. 49, dated 31.07.2009;

- By the Order of the Commissioner No. 67, dated 02.10.2009, acts of the Inspection Department on audits and inspection procedures have been approved, such as: Complaint Form; Order for Inspection; Minutes (Process-verbal) of the Administrative Inspection; Decision on Administrative Offences;

- "Notification Form" and "Guidelines for completing the Notification Form", for public and private data controllers, for fulfilling the obligation to notifying to the Commissioner's Office, approved by the Commissioner's Order No. 66 dated 01.10.2009;

- Based on Law No. 9367, dated 7.04.2006 "On the prevention of conflict of interest in the exercise of public functions", was drafted a Regulation "On preventing conflict of interest in the exercise of public functions in the Institution of the Commissioner for Personal Data Protection", approved by the Commissioner's Order No. 112 dated 24.12.2009;

- Decision of the Commissioner No. 1, dated 04.03.2010 "On detailed rules for the security of personal data";

- Decision of the Commissioner No. 2, dated 10.03.2010 "On Procedures for the administering of the data registration, data entry, their processing and disclosure" (point 6 of Article 27);

- Guidance No. 1, dated 19.02.2010 "On the permission of several categories of international transfers of personal data to a state, which does not have an adequate level of protection of personal data" (point 3 of Article 9);
- Guidance No. 2, dated 25.02.2010 "On measures to be assumed from the categories of controllers before the processing of data to be performed" (letter "c", point1 of Article 30);

- Guidance No. 3, dated 05.03.2010 "On processing personal data by Systems of Recording and Monitoring Video Cameras (CCTV) in premises, bars and other environments".

2.3 Commissioner's Acts which are actually under drafting and approval process

- Guidance to determine the time of keeping personal data, according to their purpose, in the activity of specific sectors (letter "ç" of Article 31);

- Guidance for taking security measures in the activity of specific sectors, such as police, health, education etc (letter "f" of Article 31).

3. Awareness Rising

3.1 Publications and distributions of Leaflets

Leaflets on "Introduction to the Law on Data Protection and to the Supervisory Authority"; "Guide to use social networks", which is addressed young people to get care from non-appropriate use and risks of the internet; "Guidelines for completing the notification form", to assist the data controllers on how to complete the Notification Form; "For data controller's awareness of personal data and for the compliance with the duty to notify", have been published and distributed to all concerned actors.

3.2 Seminars and trainings

Within the framework of making it public, institution building, protection of personal data and awareness rising of data controllers on their duties, responsibilities and obligations to abide to and apply the law, the Office of the Commissioner have organized various seminars in many cities of the Republic of Albania with the participation of public and private sector controllers, such as: the Municipalities,

Prefectures, Educational Directorates, Regional Directorates of Social Security, Police Departments, Regional Tax Departments, Directorates of Health Care, University, banking, mobile phone companies, large commercial centers, etc. These seminars referred to important topics on introduction to law; the duties of the data controllers when they process personal data in their work activities; on their legal obligation to notify to the Commissioner's Office the processing of personal data they are responsible; on security measures that should be paid attention to during this process, by treating safety as a continuous process, etc. Practical cases have been brought up as well by the foreign expert, Mr. Carel Neuwirt, actual Data Protection Commissioner of Council of Europe, who has assisted the Office of the Commissioner from July 2009 until October 2009, under a joint project of the Office of the OSCE and Council of Europe.

3.3 Other Activities

On 28th January 2010, the Commissioner's Office for Personal Data Protection organized on the occasion of European Personal Data Protection Day, a conference with the participation of national and international institutions, such as the Office of the OSCE, the EC Delegation, Minister of State and other interested actors and data controllers.
On this occasion, considering a whole week of data protection from 25-28 of January, several activities prepared by the Commissioner's Office took place. At the SOS-Village School in Tirana, a painting and essay competition with the theme "Protection of Privacy" with students of this school was held.

4. Executive Measures Taken

4.1 Central Register of Data Controllers

Procedures for notification of control subjects connected with the publication of information to personal data they process have started in November 2009. In this framework, Data Protection Authority has provided sending relevant documents to recall the legal obligation to notify and for registration. Sectors for which notifications have started are banking sector, healthcare, insurances, telecommunications, education and public sector.
The Commissioner's Office is in the phase of reviewing these notifications, seeking additional information from data controllers which have notified. According to legal procedures, after the registration of these entities in the "Central Electronic Registry of Data Controllers", the notified information will be published *online* at the official website, as a Register open to the public.

4.2 Handling of Data Subjects' Complaints

One of the most important activities of the Commissioner's Office pursuant to the Law no. 9887, dated 10.03.2008 "On protection of personal data", is different handling of complaints coming from the data subjects. It is understood that the Office's work only for one year has consisted in taking all legal steps to implement short-term priorities correctly and create a vision for long-term strategy to have significant impact of the implementation of the law for maximum protection of personal data, towards data subjects and data controllers.
In this context, administrative checks are conducted at the Department of Social Insurance and at the Office of Civil Status. After treatment of these complaints and checks performed, Commissioner's Office has taken the relevant legal position and the right actions by data controllers involved were taken.

4.3 Exercising of other Legal Competences and Cooperation

Pursuant to letter “a”, point 1 of the Article 31 of the Law, by which it is foreseen that the Commissioner is responsible to give legal opinions for draft laws and bylaws which touches upon the area of data protection, the Commissioner’s Office has given qualified legal opinions on laws and legal acts drafted by several public institutions such as the Directorate General of Civil Status, Ministry of Justice, Ministry of Interior, Institute for Health Care Insurance and the General Directorate of Police.

In February 2010, the Albanian DPC signed a Cooperation Agreement with the High Inspectorate for Declaration of Assets, which will work in both ways for the prevention of conflict of interest and for the protection of privacy and processing of personal data.

In May 2010, the Albanian DPC signed a Cooperation Agreement with the National Centre of Registration, which will contribute to awareness rising of the controllers to fulfil the obligation to notify to the DPC, as well as to amending provisions to internal regulation of the NCR in relation to processing and security of personal data.

5. European and International Involvements

On 2-4 September 2009 in Strasbourg, France was held the following plenary meeting (the 25-th) of the Consultative Committee of the Convection for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Council of Europe. For the first time, thanks to the cooperation with the Ministry of Foreign Affairs for the accreditation of the Albanian Commissioner’s Office to this Committee, the Albanian Commissioner, Mrs. Flora Çabej (Pogaçe), attended this meeting with the full capacity of the official member to this committee with the right to vote.

On 3 November 2009, in Madrit, Mrs. Çabej, the Commissioner, participated in the Francophone Conference. Nearly all francophone countries introduced relevant legislation in the field of protection of the rights of children and to future projects in this area. It should be mentioned that the Albanian Commissioner for protection of personal data gained full membership and rights to this Francophone Association of Data Protection Authorities.

On the dates 4-6 November, Madrid, the 31st International Conference of Data Protection Authorities followed. This big conference consisted mainly in active contribution to the progress of the development of privacy and personal data protection, the balance between security and privacy, prevention and response regarding security breaches, etc.

During the following Conference of European Data Protection Authorities (Spring Conference) held in Prague, 29-30 April 2010, the Albanian Commissioner’s Office for Personal Data Protection was accredited. The Accreditation Committee unanimously accepted the request, after receiving the official request of the Albanian DPC, presented by the Czech Republic’s Office for Personal Data Protection.

6. Trainings of the Commissioner’s Office Staff

Beneficiary of a very valuable foreign experience given the period July – October 2009, have been in particular the staff of the Commissioner's Office. Foreign expert located in the office premises, Mr. Carel Neuwirt, trained the staff twice a week by delivering very accurate presentation on important topics on data protection, reflecting the experiences and best practices of most developed countries in this field, and has assisted in drafting some administrative acts and necessary legislation to implement the law accordingly with efficiency and to organize the institution to exercise its duties and competences consistently.

Conclusion of all procedures for participation in Study Visits and practical training

to the corresponding Personal Data Protection Offices: in Czech Republic 27-28 August 2009, in Sweden 01-02 December 2009, in Portugal 10-11 December 2009, in Slovenia 15-16 December 2009 and in Italy 21-22 December 2009. The programs of these visits specifically relate to all spheres of personal data protection and privacy.

CROATIA

REPORT
on the activities of the Croatian Personal Data Protection Agency
in the period between September 2009 and May 2010

IPA-Project "Strengthening of the capacities of the Croatian Personal Data Protection Agency"

The Croatian Personal Data Protection Agency (further in text: Agency) shall implement the project through the twinning and equipment procurement. Additional activities aiming at strengthening of Agency's advisory and supervisory role and pilot-projects in the health, telecommunication and marketing sector have newly been introduced in the project. In order to ensure the best possible cooperation with the state bodies, the Ministry of Interior and the Ministry of Justice have become stakeholders in the project. The project will also aim at raising of citizens' awareness on the need and importance of personal data and privacy protection as one of the fundamental human rights via promotional campaigns and through organisation of a seminar on personal data protection on a national level.

The Spanish Data Protection Agency (Agencia Española de Protección de Datos) has been chosen as a twinning partner. However, many other personal data and privacy protection experts from other countries will be involved in the project.

By providing new IT-equipment the Agency tends to improve its IT infrastructure and business processes. It also strives to achieve a full harmonisation with the highest international information security standard, ISO 27001. Besides introducing a multilevel security model, special attention will be given to Agency's website, services and possibilities of a direct communication with other data protection commissioners via website.

In the framework of the **Leonardo da Vinci Partnership 2010** the Agency has applied for two projects:

- **"Raising awareness of the data protection issues among the employees willing to work in the EU"** in cooperation with the Polish, Hungarian and Bulgarian data protection authorities; and
- **"Perception of data protection and privacy issues by children and youth"** in cooperation with the Polish and Hungarian data protection authorities.

Inspection

In the reporting period the Agency has carried out ex officio inspections on personal data processing directly at the premisses of data controllers as well as inspections on personal data filing system notifications to the Central Register. The Agency has also conducted inspections on the information security measures undertaken for personal data protection.

The inspection activities were carried out in the sector of state administration, local administration and self-administration, economy, education, health, social care, telecommunications and others. A special attention has been paid to video surveillance in schools, inspections in the health sector with emphasis on data storage methods and special measures of technical protection of special categories of personal data as well as to inspections in the telecommunication sector.

Raising awareness on the need for personal data protection

Expert meetings

The Agency takes regularly part at various types of expert meetings either as a guest or as an organiser. In September 2009 Agency's representative participated in HIDE Workshop in Ljubljana (Slovenia) with the presentation "Public interest - data protection, practice and experience in Croatia", in November 2009 at the Round table "Is there any privacy on the Internet?", which has been held within a conference on Internet Revolution and at the 7. conference on personal data protection and identity management.

Seminars for data controllers

The Agency was co-organiser of seminars for data controllers, which have been organised in some bigger centers throughout Croatia, in order to achieve the best possible results when it comes to complying of data controllers with their legal obligations.

Education of citizens

The Agency is conducting systematical education activities of Croatian citizens on their rights to personal data and privacy protection. The lectures are being organised under the name "Personal data and privacy protection in the Republic of Croatia" in cooperation with civic organisations and NGOs for human rights. Through such an interactive approach, citizens acquire better understanding of the problem of personal data protection, which is contributing to Agency's work, giving it further guidelines for improvement and development of the educational platform for Croatian citizens on personal data and privacy protection.

European Data Protection Day

On 28th January 2010 the Agency has celebrated for the 4th time in a role the European Data Protection Day. Various activities such as Open Dor Day at the Agency and Info-desk at one of the most frequent shopping centers in Zagreb have been organised. In the center of the activities was a Round table organised for relevant experts from all state bodies and institutions, NGOs and media and the participants themselves were the representatives of the Agency, of the Ministry of Interior and of Polytechnic of Zagreb on the following topic: "Personal data protection in the use of information-communication technologies".

Cooperation with media

The Agency has in the reporting period received many different inquiries and questions such as: about the Agency, collecting and processing of personal data from shopping centers, insurance companies and political parties, social networks, national ***identification number and personal identification number, biometrical passports, video surveillance at work and in schools, recording of phone conversations by user centers of banks and telecommunication***

operators, use of technological gadgets and softwares (e.g. Partnerlocator), unlegitimate and unsolicited data collecting and processing, publication of the Croatian war veterans register, use of personal data for marketing purposes, violation of the health ***data secret, European Data Protection Day, registration of prepaid cards for mobile phones, telephone numbers in the telephone diary, education for citizens on personal data and privacy protection etc.***
The Agency has replied to all questions raised by the media either by means of interviews, written answers, press releases or publication of Agency's opinions and decisions on the official web site.

CYPRUS

In October 2009 the Council of Ministers of Cyprus issued a decision adopting the Commissioner's proposal with regard to the designation of a data protection officer in every government department.
In light of the above decision the Commissioner's Office is the competent authority for the training and guidance of all designated data protection officers.
As of 10/5/2010 Mrs Toulla Polychronidou has been appointed as the new Data Protection Commissioner.

CZECH REPUBLIC

Priorities in control activities during last period

Most of the controls including in-the-spot inspections related to the breaches of DP Act were carried out on the basis of complaints and instigations (90 %). The remaining control activities followed from the Control Plan (8 %) and the instructions of the President of the Office (2 %). It should be nevertheless noted that the last two categories of inspections involve mainly more complex control procedures. The Office also received 1458 instigations related to unsolicited commercial communication of which was resolved 1311. Only rarely the Office receives complaints against commercial communication originating abroad.
Special attention was paid to the following areas:
Public administration information systems - processing of personal data was a frequent subject of inquiries and request for consultation (controls were concerned with record of the population).
Multinational information systems - the controls were mostly initiated by the join supervisory bodies SIS and EURODAC and other EU initiative (traffic data in transport systems).
Personal data processing in the use of camera surveillance systems - the Czech DPA has applied the basic personal data protection principles published in the official DPA Position.
Information systems on the area of justice - the Czech DPA encountered personal data processing in relation to activities of judicial distrainers and administrative punishment.
In cases where the control indicated violation of the DP Act, administrative proceedings were pursued against the relevant parties for an offence related to personal data processing. In those cases were imposed fines. The party of the proceedings can lodged an appeal against the decision with the President of the Office. Recently the Office dealt with assessment within second-instance proceeding in three areas mainly: Processing data in the state administrative information systems, Assessment of camera surveillance systems, Processing personal and sensitive data in DNA databases.
Legislative activities
The Office's legislative activities were concerned to the preparation of the new codification of civil law, the work on new electronic registers of public administration and regulations related to healthcare registers.
Within provision of comments on the draft new Civil Code, the Office criticized the regulation of acquisition of records and recordings by technical means. The Office considers it positive that the draft Civil Code has been reformulated in the part concerning identification of citizens.

Regarding the system that will play a key role in the near future in the area of e-Government the Office strived to contribute in respect to privacy and personal data protection. The Office had effectively influenced questions in the area of e-

government in the Czech Republic related to the system of private data boxes in such aspects as it is the period of maintaining data in the new records that was substantially shortened, and the use of related personal identifier for other purposes that was recognized as unacceptable. The general duties concerning personal data protection will also apply in activities concerning new electronic registers and, consequently, this area will be subject to supervision by the Office. Relatively unsuccessful effort of the Office was in the area of regulations concerning healthcare registers. In the opinion of the Office, the question of concept of the registers in this area is underestimated in society; the Ministry of Health did not accept the requirement of the Office for full clarification of the concept of the registers including the purposes of their use.

Relations to foreign countries and international cooperation

Cooperation with the EU bodies and partners is a clear priority within foreign relations of the Office. An important role in the activities of the Office in relation to cooperation within the European Union was played by preparations for the Czech Presidency of the Council and contributing to its course in the first half of 2009. The main objective of participation of the Office in the preparation of related documents was to point out the aspects of personal data protection and to organically incorporate the relevant provisions in the planned activities.
During the Czech Presidency the Office organized or co-organized three important events: 1)Case Handling Workshop. 2) Czech-French meeting of top representatives of the Office for Personal Data Protection and the CNIL – Commission Nationale de l'Informatique et des Libertés; the President of CNIL Mr. Alex Türk visited the Office also from the position of the President of the Article 29 Data Protection Working Party. 3) Meeting of the Data Protection Working Party G.09 in the Council/Coreper.

Awareness Raising Activities

Overview see the PDP Day Form. The Czech Office campaigns stars at these occasion each year.

ESTONIA

Recent developments in the data protection field
May 10, 2010

Legal developments

Principal amendments were enacted in the Penalty Code of Estonia – identity theft was criminalized. According to the § 157^2 of the Penalty Code:

- the forwarding,
- granting of access or
- using

the personal data of other person without his/her consent, but with the purpose to create incorrect image of this person and in case when the using of these data cause damage for the person's rights or interests, shall be punished with financial punishment or prison sentence up to 3 years.

Data protection Day

On the 27th of January 2010 Estonian Data Protection Inspectorate celebrated Data Protection Day with the fourth consecutive conference. This year the focus was on processing personal data for employment purposes. The screening of employees' e-mails and monitoring their Internet behaviour, but also the using of video surveillance were extensively discussed. The conference initiated discussions in media. Inspectorate had positive feedback. As a result of the conference the Inspectorate is planning to issue detailed guidelines about the right for privacy in the employment relationships. For the record - Recommendation No. R (89) 2 of the Committee of Ministers to member states on the protection of personal data used for employment purposes has been translated into Estonian and is available at our website.

Other issues

For the third year the inspectorate chooses priority topics and issues guidelines on these matters. The guidelines (2009) are available only in Estonian.

1. Processing of personal data with regard to election campaigns.
2. Processing of personal data by the financial institutions.
3. Processing of personal data with regard to genealogical researches.
4. Processing of personal data with regard to scientific researches.
5. The use of national ID-codes.
6. Disclosure of personal data of the debtors of utility costs.
7. The right to ask your own data.

FINLAND

INFORMATION ON RECENT DEVELOPMENTS IN THE DATA PROTECTION FIELD IN FINLAND SINCE THE 25th PLENARY MEETING OF THE T-PD

1. Legislation

Act on the Protection of Privacy in Electronic Communications

The amendment to Act on the Protection of Privacy in Electronic Communications entered into force on 1 June 2009. The amendment gives association subscribers the right to process identification data in order to prevent and detect illegal use of fee-based information society service, communications network or communications service or business espionage as referred to in the Criminal Code (Rikoslaki 39/1889).

During the year under review, the amendments required by the directive (2006/24/EC) were entered in the Act on the Protection of Privacy in Electronic Communications (516/2004). The legal obligation to store telecommunications identification data entered into force on 15 March 2009.

The new Act on the Population Information System and the Identification Services of the Population Register Centre (Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 661/2009) entered into force on 1 March 2010.

2. Major case law

2.1. The Court of Justice of the European Communities (the Grand Chamber) gave its ruling on the publication of data on earned income on 16 December 2008. The matter pertained to the scope of application of Directive 95/46/EC, the processing and mobility of personal data on taxation, protection of individuals and freedom of speech.

The Supreme Administrative Court gave its judgement on 23rd September 2009, KHO:2009:82. The Court sent the case back to the Data Protection Board, obligating the Board to send a refusal to Satamedia on their continued publishing of the data. The refusal covered both the publications and the SMS service. The Court stated in its judgement that Article 2.4 of the Finnish Personal Data Act is not in line with the directive in the way the ECJ has interpreted the scope of application of the directive. The Court reached its resolution through two considerations: the balance between freedom of speech, and protection of private life. The Court pointed out that the balance requires that for the part of freedom of speech, information provided to the audience has to have importance in society and not only serve the needs of curiosity. For the part of the purpose of journalism, the Court paid attention to the actual manner of producing these ”newspapers”. Since the database (register) was printed as such, it couldn’t be created only for journalistic purpose. The court’s decision was that Veropörssi had no legal basis to process personal data and thus the text message service was also illegal. The Court did not tackle the issues of the taxation data as such or the question of the balance between freedom of speech and privacy. The

service provider of the SMS service notified the DPA on 28.9.2009 that they would stop the service on 30.9.2009 on the basis of evident illegality. In practice, Finnish newspapers will, in the future, also publish this kind of personal data about persons who have the capacity for social importance. Future amendments to the Finnish Personal Data Act on the inconsistency of Article 2.4. will be prepared by the Ministry of Justice.

The Data Protection Board has, in its decision dated 26 November 2009, prohibited Satakunnan Markkinapörssi Oy from processing data pertaining to earned and capital income and assets of natural persons to the extent and in the manner that took place in connection to 2001 tax records. Moreover, the Data Protection Board has prohibited Satakunnan Markkinapörssi from submitting data they have collected and stored pertaining to earned and capital income and assets of natural persons through an SMS service or for any other purpose. The Data Protection Board has also prohibited Satamedia Oy, due to infringement of the Personal Data Act (Henkilötietolaki 523/1999), from collecting, storing and submitting further data pertaining to earned and capital income and assets of taxpayers received from Satakunnan Markkinapörssi Oy register and published in printed form in a publication entitled Veropörssi.

2.2. The competent Data Protection Board also gave its decision on the matter initiated by the Office of the Data Protection Ombudsman on the authentication of quick loan applicants via mobile phone. In its decision, the Data Protection Board ruled that the practice whereby the creditor identifies the loan applicants solely on the basis of the name, social security number, address and telephone number data provided via a text message that is accepted as a loan application, cannot be considered as a sufficiently reliable practice. Therefore, the Board prohibited the respondent, who followed an authentication process commonly used in the sector, from processing personal data in the aforementioned manner. The respondent complained about the decision of the Data Protection Board to the relevant appeal court. Partly due to this case, a proposal to enact a general law on authentication was put forward in Finland. The overall reform of legislation on consumer credit was implemented with the amendment of the chapter 7 of the Consumer Protection Act (Kuluttajansuojalaki 38/1978) which entered into force on 1 February 2010.

3. Specific issues

Surveys conducted

During the year under review, the Office of the Data Protection Ombudsman conducted several surveys.

During summer 2009, the Office of the Data Protection Ombudsman implemented a sector-wide survey on market and opinion polls. Questionnaires sent to a hundred companies charted procedures pertaining to polls and the extent of personal data processing. Particular attention was paid to the upholding of civil rights. The sector survey showed that some of market and opinion poll makers know the requirements of the data protection legislation, and take them into account in their activities. However, some of the answers demonstrated a degree of ignorance with regard to data protection competence. Citizens' names

and contact information are acquired for research purposes, especially from electronic directory and directory inquiry services, as well as official registers. Since in Finland it is possible for the Data Protection Board to issue a permit to process personal data and set special conditions for the processing, the Office of the Data Protection Ombudsman conducted a survey on how well permit recipients followed permit decisions and their conditions. The survey results showed that permit conditions are followed well.

ITALY

Information on recent developments at national level in the data protection field

Implementation of Directive 95/46/EC and 2002/58/EC and other legislative developments

The regulatory framework related to implementation of directives 95/46/EC, 2002/58/EC and 2006/24/EC did not undergo major changes in 2009. However, Parliament enacted a few measures that led the DPA to voice its concerns as for their possibly negative impact on the protection of personal data.

More specifically, Act no. 15/2009 on the enhancement of productivity in the public sector introduced an amendment to Section 1 of the DP Code (196/2003), whereby "*The information on performance of the tasks applying to any entity that is in charge of public functions including the respective evaluation data shall not be the subject of privacy safeguards*." The DPA drew Government's attention to the advisability of moving this provision to the chapter in the DP Code that regulates processing operations by public bodies and also questioned its conformity with both Constitutional and Community law – as certain items of information and whole categories of data subject are placed outside the scope of protection afforded by data protection legislation.

Section 130 and Section 162 of the DP Code were also amended in 2009 to enable the companies that had created databases by extracting information contained in public telephone directories prior to 1 August 2005 to continue using such data for promotional purposes; a public opt-out register was also introduced and placed under the DPA's supervision. It should be recalled that on 28 January 2010 the European Commission sent the Italian Government a letter with a request for information on the above amendments as it found that the latter were in breach of directives 2002/58 and 95/46 – this being the first step in the infringement procedure envisaged by Community law.

On a different note, reference should also be made here to Act no. 69/2009, which introduced various requirements to foster computerisation of public administrative agencies and the online publication of judicial decisions. Data protection-relevant provisions are contained in section 21 thereof, which requires public administrative bodies to publish senior officials'/executives' annual salaries, CVs, e-mail addresses and office phone numbers on the respective web sites; section 32, whereby the requirements applying to publicity of administrative decisions and instruments are fulfilled by publication of such decisions and instruments on the relevant agencies' websites; section 36, which is aimed at expediting the implementation of the "public connectivity system" to ensure "full interoperability of databases and census registers" in order to afford better services to citizens and enhance efficiency of the public administration; and section 45, which amends the civil procedure code by allowing judicial decisions to be also published on Internet websites.

Another important piece of legislation enacted in 2009 was aimed at implementing the provisions contained in the Prüm Treaty by setting up the national DNA database and laying down the relevant procedural mechanisms (Act no. 85/2009). The national DNA database will be set up at the Ministry for Home Affairs and include DNA profiles obtained in the course of judicial proceedings along with those of missing persons and/or their blood relatives, unidentified corpses and human remains, and individuals placed under judicial measures restricting their personal freedom. The Italian DPA will be in charge of supervision over this database. Most of the suggestions and amendments proposed by the DPA were taken on board, in particular those aimed at ensuring respect for the individuals' dignity and proportionality of processing operations; additional safeguards will have to be set forth via secondary legislation, to be adopted after consulting and/or in agreement with the Italian DPA. However, the recommendations concerning the overly broad scope of the provisions on coercive taking of DNA samples and the excessively long data retention periods were not dealt with satisfactorily.

Written Submissions to Parliament – A written submission to Parliament was made in December 2009 concerning advisability of passing ad-hoc legislation to regulate *whistleblowing* (integrity lines) in the corporate sector. The DPA drew attention in particular to the need for regulating the lawful use of personal data collected via the "good faith" reports lodged by whistleblowers as well as access by data subjects to their own data as collected in this manner.

B. Major specific issues

Raising Youths' Awareness and Social Networks

The Italian DPA decided to launch an initiative targeted to students on the occasion of the European privacy day (28th January). The initiative was termed "Cinema & Privacy" and lasted four days; it was aimed at raising youths' awareness of the importance of protecting privacy in today's society and of the need for learning how to protect one's privacy. Movies chosen as particularly relevant in addressing privacy issues from different standpoints were shown at the Conference Room of the Italian DPA. Each movie was introduced by one of the four members of the DPA's collegiate panel as well as by a video created on purpose by the Italian DPA to describe – again with the help of movies – minor and major "intrusions" into our private sphere. Students from high schools in Rome were invited to the shows and called upon to discuss and exchange views Additionally, a booklet was produced by the DPA in 2009 to provide guidance (especially to youths) in dealing with social networks and making a knowledgeable use of their potential. The booklet, called "Social Networks: Watch out for Side Effects" was made available for free in the main Italian post offices. This initiative was aimed at helping both experienced and inexperienced users to take full advantage of the potential inherent in these innovative communication tools without endangering their private and professional lives.

Database Security

The DPA reviewed and recast (on 25 June 2009) a decision dated 28 November 2008 to enhance the safeguards for data subjects in connection with the activities performed by "system administrators" – a concept that is actually not defined

expressly by the Italian law. The new text was meant to clarify various points, partly to take account of queries lodged with the DPA. The requirements set forth by the DPA had to do more specifically with access logging (systems must be in place to log accesses to processing systems and electronic databases as performed by system administrators, e.g. via timestamps and event descriptions, without recording the activities performed by system administrators following their access); supervision by data controller on the activities performed by system administrators (to verify that they are compliant with the organisational, technical and security measures provided for in data protection legislation); drafting of a list of system administrators and their features (containing information to identify system administrators including a list of the functions committed to them), which should be reported by each data controller in an internal document that should be made available for inspection by the DPA. The DPA highlighted the need to take special care in assessing experience, skills, and reliability of any individual that is entrusted with system administrator functions, in particular to ensure full compliance with data protection legislation as also related to security.

Sensitive Data and Health Care

Online Examination Records. The Italian DPA provided guidance on the use of personal data in connection with "online access to examination records". The Guidelines are meant to lay down a specific, unified framework of safeguards for citizens, in particular as for the optional nature of the online access to examination records. Data subjects should be permitted to freely decide whether to access the online examination records service – based on a specific information notice and after obtaining ad-hoc consent for the processing of personal data related to the service in question; they should be enabled in all cases to continue collecting such examination records on paper at the individual health care provider(s). Specific technical arrangements are set forth to ensure appropriate security measures: secure communication protocols based on encryption standards for electronic data transfers, including digital certification of the systems delivering network-based services; suitable arrangements to prevent acquisition of the information contained in the electronic file if the latter is stored in local and/or centralised caching systems after being consulted online; short-term (maximum 45-day) availability of the online examination record.

Guidelines on the Electronic Health Record and the Health File. The Guidelines suggest that the Electronic Health Record should be set up by prioritizing solutions that do not entail duplication of the medical information created by the health care professionals/bodies that have treated the given data subject.

Since the medical data and documents contained in a EHR are collected from different sources, the appropriate measures should be taken to allow tracing back the entities responsible for creating and collecting the data and making them available via the EHR - also with a view to accountability. In particular, taking account the circumstance that separate clinical records are at issue, it should be ensured that each entity that has created/drafted those records continues to be, as a rule, the sole data controller in their respect.

The data subject must be in a position to freely decide whether an EHR/HF should be set up by including the medical information concerning him; his

consent must be given on a separate, specific basis; suitable explanations should be provided to data subjects. "Partitioning" of consent should be envisaged to enable data subjects to indicate their wishes. Specific limitations are laid down on the purposes served by the EHR/HF, by clarifying that processing of personal data via an EHR/HF is only aimed at prevention, diagnosis and treatment activities in respect of the data subject; accordingly, it should only be performed by health care practitioners. This modular approach allows, for instance, selecting the health care information that can be accessed by the individual data controller authorised to access the EHR as a function of the respective sector of practice - e.g. in the case of an oncology network made up of operational units specialising in cancer treatment. Similarly, a few categories of practitioner such as pharmacists may only access such data (or data modules) as are indispensable to administer drugs.

Public Transparency and Online Posting of Medical Data. The DPA required medical information relating to over 4,500 disabled individuals to be taken down from the institutional website of a Region and also initiated a sanction proceeding against the competent local authority. It was found that the list of disabled individuals that had been granted an allowance by the Region to purchase a PC could be browsed freely online – including their names, disabilities, places of residence and birth dates. The DPA reaffirmed that medical information may not be disseminated unrestrictedly and that public transparency requirements should not override data protection obligations as applying to public bodies – in particular, the obligation not to disclose excessive information compared to the specific purposes.

National and Regional Registries of Mammal Prostheses. The DPA objected to the setting up of a registry including the names of women that have had mammal prostheses implanted, in connection with a governmental bill related to breast surgery. It was recalled that the monitoring of plastic surgery could be ensured by respecting anonymity of the individuals operated upon and using statistical codes and tools. The DPA pointed out the need for detailing who would be entitled to access the registry and for what specific purposes, since the wording used in the bill was excessively vague.

Businesses

Mergers and Split-ups – The DPA clarified what obligations should be fulfilled by companies in cases of mergers (by absorption and/or amalgamation) and split-ups to ensure compliance with privacy legislation. In particular, the companies involved should notify their customers, employees and suppliers of the name(s) of the new data controller and data processor(s), if any; to that end, simplified mechanisms may be used such as posting the information initially on the companies' websites and providing individual information to their personnel thereafter.

Business Information Services – The DPA exempted various companies providing business information services from the obligation to provide information notices to all data subjects, as it found that this obligations entailed a disproportionate effort compared to the interests at issue; however, the DPA

required effective alternative measures to be deployed by the companies involved.

Anti-Money Laundering Legislation and Financial Brokers – It was clarified that financial brokers belonging to the same corporate group may lawfully communicate and process personal data without the data subjects' consent in connection with reporting "suspicious" transactions to the extent this reporting activity is in line with anti-money laundering legislation and is aimed exclusively at countering money laundering.

Company Registers – The DPA clarified that the DP Code does not place any limitations on access by shareholders to the personal data contained in company registers, nor is it in conflict with openness of corporate activities. Shareholders are entitled to know addresses and personal information related to other shareholders in order to contact them and defend their legitimate claims.

Telephone and Electronic Communications

Telemarketing. The possibility to further use (until 31 December 2009) the data contained in telephone directories set up prior to 1 August 2005 for marketing purposes without the data subjects' consent, introduced by Act 14/2009 (see 12th Annual Report), had prompted the Garante to clarify the limitations applying to compilation and use of such data via an ad-hoc decision (March 2009). More specifically, the DPA had required, inter alia, the data controllers wishing to avail themselves of the above possibility to provide proof that the data had been actually extracted from telephone directories compiled prior to 1 August 2005 and to only use the data for contacting subscribers for promotional purposes, i.e. it was clarified that marketing companies were prohibited from contacting subscribers in this manner in order to surreptitiously obtain their consent to use their data for promotional activities also after 31 December 2009. Following the amendments made to the DP Code by Act 166/2009 (see above, "Legislative Developments"), which extended the deadline for using the data in question and also provided for the establishment of an "opt-out register" applying to telemarketing by 25 May 2010, the DPA decided to extend enforceability of the requirements laid down in the above decision accordingly. On this same note, the DPA rejected the practice of using randomly created phone numbers to contact subscribers for promotional purposes, as it found that such numbers, though created via randomized mechanisms, do represent personal data under the Italian DP law and as such enjoy all the safeguards provided for in the law – including the need to obtain the subscribers' prior informed consent to using them.

Customer Profiling – Specific obligations were imposed by the DPA (decision dated 25 June 2009) on the providers of publicly available electronic communications services as regarded profiling of their customers. A detailed analysis was carried out, which led to distinguishing among different categories of profiling and requiring data controllers to make different arrangements. In particular, two scenarios were envisaged: 1. profiling based on "identifiable" personal information, which requires the data subjects' free, informed, specific consent; 2. profiling based on "aggregate" personal information, i.e. aggregate data derived from identifiable personal information, which requires either the data

subject's consent or, where this has not been obtained, a prior checking application to be lodged with the DPA by the data controller pursuant to Section 17 of the DP Code. In the latter case, account will have to be taken of the aggregation level (i.e. the level of detail of the aggregated data) and the technical arrangements applying to the processing. Additional obligations such as notification to the DPA and the provision of appropriate information to data subjects were also laid down.

Journalism

On several occasions, the DPA had to step in to safeguards privacy rights vested in children. In particular, a few newspapers were prohibited from publishing names and pictures of children involved in reported cases and/or providing information that would allow identifying those children. In child abuse cases, the DPA recalled that it was necessary to safeguard the privacy both of the children and of the other individuals involved – by refraining from disclosing the child's age, sex and place of residence; the relationship between child and suspect, if any; or the father's job or profession.

Several requests were lodged with the DPA to have data and pictures available on the Net (e.g. via Google, Emule, YouTube, forums, and blogs) erased. In some cases the DPA could not take any steps directly because the controller of the Internet website was not resident in Italy; conversely, in other cases instructions were provided to the data controller to erase the pictures/data considered to be in breach of the law.

Two cases handled by the DPA concerned newspapers and TV channels that had published pictures taken directly from Facebook when commenting on the death of two individuals, even though the pictures in question did not correspond to the deceased individuals but rather to namesakes. The DPA found that publication of those pictures was in breach of data protection legislation as accuracy of the information collected had not been checked thoroughly and erroneous personal information had been disseminated. It should be pointed out that an increasing number of complaints relate to the processing of personal data extracted from Facebook profiles; misuse of personal information and defamation are the most frequent complaints in this regard.

Another important decision in this area reiterated that filming and using images of individuals within private premises without the individuals' consent was unlawful. The DPA prohibited the dissemination/publication by whomsoever of images acquired and/or obtained in breach of the safeguards applying to private premises, in particular considering the privacy-intrusive techniques implemented to capture those images, the lack of consent by the relevant data subjects, and the exclusively personal nature of the activities shown in those images.

Formal Complaints

In 2009, there were 360 decisions on formal complaints (which are specifically regulated and time-barred). Like in previous years, most of them concerned banks, financial companies and credit reference agencies. However, the most interesting issues had to do with the voice as personal data, the exercise of data

protection rights concerning deceased persons, and the posting on-line of publicly available information.

Voice as a personal data. The DPA granted the complaint lodged by a consumer against a telephone operator that had implemented a contract based on a "verbal order". The DPA found that the recording of the call should be made available to the data subject requesting it, as it was not enough for a summary transcript of the relevant contents to be provided. The rights set forth in data protection legislation can be exercised by data subjects also in respect of sound and image data, which are personal data; accordingly, the right to access the personal data contained in the "verbal order" is only fulfilled by making available the recording of the call so as to access the specific voice data.

Clinical records of a deceased person. The DPA granted the complaint lodged against a university hospital that had failed to reply to several requests for obtaining the personal information related to the treatments that the complainant's partner had undergone. The DPA found that the partner of a deceased person had the right to access that person's clinical record in order to establish judicial claims on the conduct held by the caregivers. Under section 9(3) of the DP code, the right to access personal data related to deceased persons "may be exercised by any entity that is interested therein or else acts to protect a data subject or for family-related reasons deserving protection" – and the complainant had clarified that the data in question were necessary with a view to taking legal action to establish the caregivers' flawed and/or negligent conduct.

Online publication of the resolutions by a municipal body. The DPA ordered a municipality to erase the complainant's address from a resolution that had been posted on the municipality's institutional website and could be retrieved by means of external search engines. The complainant had claimed that blanking his address from the resolution was not in conflict with the transparency of electronically published public instruments and records. The DPA pointed out the need to carefully select the personal data to be published in this manner, as their publication should prove necessary under the specific circumstances for the purposes sought by the given measure – in compliance with the principles of relevance and non-excessiveness and by balancing the right to privacy with the obligation to ensure publicity of the decisions made by a local authority. Publishing the resolution at issue in full impacted disproportionately on the complainant's rights as it resulted into disseminating irrelevant information on the web.

Inspections

The DPA was strongly committed to inspection activities also in 2009. Based on six-monthly inspection plans, 449 inspections were carried out as a whole. In performing such inspections, the DPA can avail itself of a specialised corps within the Financial Police, which is in charge of checking compliance with the requirements concerning notification, information notices, security measures, and enforcement of the resolutions adopted by the Garante. Forty-five inspections were carried out directly by the inspection department at the DPA concerning, in particular, public bodies that access the information system of the Revenue

Service (13); companies providing databases to third parties for marketing purposes (10); and telephone operators as for the retention of traffic data for customer profiling purposes (9). As for the inspections performed by the Financial Police upon the DPA's instructions (which specify data controller and scope of the inspection), the following areas were covered: private hospitals (35); public hospitals and nursing homes (35); public transportation companies (30); casting companies (26); suppliers of building materials (25); golf clubs (25); businesses controlled by municipalities dealing in waste collection (20), sales of methane (20), and sales of water (20); tourist harbours (20); betting agencies (15); ski lift companies (10); companies selling electronic ware (10); pharmacies (20); companies that notified the use of databases on creditworthiness/defaults (20); other entities as per the specific requests made by legal departments at the DPA (83).

Following the inspections, 43 reports were preferred to judicial authorities and 368 procedures initiated to issue administrative sanctions; additionally, in about 150 cases proposals were submitted to the competent legal departments at the DPA to impose obligations on the data controllers aimed at bringing processing operations into line with the law.

One-hundred and seventy sanction procedures were finalised in 2009 and a total of 1,572,432 Euro was levied via the relevant fines.

As for criminal cases, several had to do with the failure to take minimum-level security measures (24); unlawful data processing operations (7), the provision of untrue statements and information to the DPA (6), and non-compliance with orders/measures issued by the DPA (4) were also detected.

LATVIA

Major developments in the data protection field in 2009

Elaboration and amendments to legal acts:

- **Personal Data Protection Law**

Personal Data Protection Law was amended on 12 June 2009 and the main changes were related to exceptions for notification of personal data processing in Data State Inspectorate, obligation to submit the request to controller in case of possible breach of Personal Data Protection Law before the complaint is submitted to Data State Inspectorate. The amendments also foresee that Data State Inspectorate no longer accredits internal and external data processing auditors.

Furthermore the drafts of two additional amendments to Personal Data Protection Law have been elaborated:

- regarding exception to conclude the agreement on data transfer to third countries in law enforcement sector if it concerns international cooperation on national security and in the field of criminal law;

- regarding decisions of Data State Inspectorate that foresee the interception or interruption of data processing, the amendment foresee that the decisions could not be reprieved in case of an appeal decision.

- **Law on Data State Inspectorate**

In order to ensure a complete independence of Data State Inspectorate of Latvia, the elaboration process of draft Law on Data State Inspectorate has been finished. Due to the necessity of reviewing the necessary means for the functioning of the independent data protection authority in correspondence with the economical situation in Latvia, the draft law was updated in 2009. The announcement of the Law is intercepted until the European Community Court decision on the independence of German data protection authority will be taken.

- **Regulation on data transfer to third countries**

In 2009 Data State Inspectorate of Latvia continued the activities on elaboration of the Regulations of the Cabinet of Ministers on Standard requirements for agreements for personal data transfer to third countries. The regulation implements the requirements regarding content of contracts stipulated in Commission's Decisions 2001/497/EC and 2004/915/EC on Standard Contractual Clauses for the transfer of personal data. The Regulations will be

announced after the amendment in Article 28 Personal Data Protection Act, the amendment is already elaborated and is sent to the Parliament.

- Regulation on Requirements on Audit report on personal data processing in state and local government institutions

The budgetary cut and reduction of functions and administrative capacity of Data State Inspectorate caused the amendments to Personal Data Protection Law that came in to force on 1 July 2009. Those amendments foresee that accreditation of personal data processing auditors is no more essential; instead of this stating that the requirements for audit reports are determined with the Regulations of the Cabinet of Ministers. In 2009 Data State Inspectorate has elaborated the Regulations of the Cabinet of Ministers (17 November 2009 No.1322) "Requirements on Audit report on personal data processing in state and local government institutions" that came into force on 25 November 2009. The regulation specifies the content of audit reports on personal data processing in state and local government institutions should be submitted to Data State Inspectorate once in two years and should contain the risk analysis of personal data processing, evaluation of compliance with legal acts regarding personal data processing for each data processing purpose separately, the conclusions with rating of the risks and recommendations on improvements.

- **Law on Information Society Services**

Due to amendments in Law on State Budget for 2009 and budgetary cut of Data State Inspectorate, Data State Inspectorate has elaborated the amendment to the Law on Information Society Services. The amendments foresee that Data State Inspectorate is obligated to start an investigation in case when the person has received 10 commercial communications from one sender within period of one year; however it doesn't exclude the self initiative investigations of the DSI.

- **Electronic Communication Law**

In Accordance with Article 4 of Electronic Communications Law protection of personal data in the electronic communications sector shall be supervised by Data State Inspectorate. In 2009 Data State Inspectorate faced the problem regarding different interpretation of legislation on the rights of Data State Inspectorate on access to retention data. Due to necessity on solving the problem, Data State Inspectorate has elaborated the amendment to Electronic Communications Law and it is expected that the amendment will come into force in 2010.

Major specific issues:

- **Data Protection Officers**

In 2009 Data State Inspectorate of Latvia has organized four examinations for Data Protection Officers and certificates have been issued to seventeen data protection officers who represent both - the private and governmental

sectors. The training of Data Protection Officers in 2009 is carried out by private sector.

- **Elaborated recommendations and guidelines**

In 2009 Data State Inspectorate has elaborated "Recommendation on Data Transfer to Third countries". Taking into account the number of questions received by Data State Inspectorate regarding clarification of the Article 28 of Personal Data Protection Law that regulates personal data transfer to third countries, Data State Inspectorate has elaborated the recommendation on this issue.

With the aim to clarify the personal data processing notification process in Data State Inspectorate the guidelines for controllers was elaborated, especially taking into account the recent amendments on Personal Data Protection Law regarding exceptions from notification.

- **Data Protection Day 2009**

In Data Protection Day 2009 Data State Inspectorate carried out activities regarding personal data protection regarding photography's and personal data processing carried out by photographers (amateurs and professionals). The discussion with Latvian associations of photographers took a place and representative of Data State Inspectorate participated in a seminar for photographers where the lecture/ workshop regarding legal liability of photographer will be held. One of the issues discussed was – how to ensure privacy in photographers' daily work. Data State Inspectorate introduced the photographers with guidelines regarding personal data protection.

Most common violations of personal data processing where related to:

- **publishing personal data on internet;**
- **data processing of credit reference agencies and data transfer to third persons;**
- **use of personal data of another person for identification purposes in cases of administrative breaches;**
- **video surveillance;**
- **data processing carried out by house maintenance services.**

The specific case that drew the attention of media was video surveillance that covered the fitting room areas in large supermarket chain. In 2009 the amount of cases increased when persons were using personal data of another person instead of their own personal data during the process when the identity of the suspected persons was clarified by police.

At the national level Data State Inspectorate participated in discussions related to several topics, for example:

- amendments to legal acts related with budgetary cut (including the reduction of functions and administrative capacity of Data State Inspectorate);
- data processing in state level systems for education purposes;
- the use of body scanners in prisons;
- publication of court decisions and data anonymisation;
- data processing regarding consumer credits and collection of debts;
- access to data bases in process of vehicle insurance purchasing (online-purchasing systems).

LITHUANIA

COUNTRY REPORT OF THE REPUBLIC OF LITHUANIA ON RECENT DEVELOPMENTS AT NATIONAL LEVEL IN THE DATA PROTECTION FIELD

1. Recent National Developments – legal framework
1. Laws
1.1. The New Wording of the Law on Legal Protection of Personal Data
1. The Law Amending the Law on Legal Protection of Personal Data (hereinafter – LLPPD) entered into force on the 1st of January 2009.
The new wording specifies provisions of the LLPPD regulating the processing of personal identification code. According to the new wording the data controllers that are processing by automatic means personal health related data for the purposes of health protection and that are processing personal data for scientific medical research purposes have to notify the State Data Protection Inspectorate (hereinafter – SDPI) and apply for the prior checking. The term "video surveillance" has been defined and regulations regarding the processing of personal image data, the processing of personal data for direct marketing and for solvency evaluation purposes was adopted. Also regulations regarding the status of a person or of a unit, responsible for data protection and the procedure for handling complaints were adopted. The new wording of the LLPPD establishes the independence of the SDPI functioning as a supervisory institution changing appointment procedure of the Head of the Inspectorate. According to the LLPPD the Director of the SDPI shall be a civil servant, the head of the institution, taken into service through competition for the period of office of five years and shall be dismissed by the Prime Minister in accordance with the procedure established in the Law on Civil Service. A person may be appointed to the post of the Director of the State Data Protection Inspectorate for not more than two periods.
Despite that new version of the Law entered into the force only on the 1st of January 2009, a new Draft Law Amending the LLPPD is currently given to the Parliament for considerations. The Draft of the Law states that it should not be applicable for the data of deceased persons. Also it envisages a change of status of the Director of the SDPI. According to the Draft Law the Director of the SDPI shall be appointed by the Government of the Republic of Lithuania for a term of five years and dismissed from office by the Government upon the nomination of the Minister of Justice. Another changes regarding of the processing of personal data for managing of debts and for solvency evaluation purposes were introduced. Special categories personal data suchlike data about not expired convictions for crimes against property, property rights and property interests, crimes against economy and business order as well as crimes against financial system also crimes against government order relating to forgery of documents or measuring devices, data about convictions for serious crimes might be processed for solvency evaluation purposes on condition that the data subject has given his consent. Data on the services rendered, their performance and

proper fulfilment cannot be stored for a period longer than 10 years from the date of fulfilment of these obligations.

1.2. The amendments of the Law on Electronic Communications

The amendments of the Law on Electronic Communications transposing the 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 entered into force since 16th March 2009. The law foresees that the traffic data of the subscriber or registered user of electronic communications services may be stored no longer than 6 months from the date of communication, except for cases, where the bill is lawfully disputed or the data are necessary for debt recovery also in cases referred to in Article 77(2) of this Law. In pursue of ensuring the access to data in cases of a serious and extremely serious crimes, as they are described in the Penal Code of the Republic of Lithuania, where such information is necessary for the purposes of investigation, detection and prosecution of criminal acts, the providers of public communications networks and/or public electronic communications services must store traffic data for a period of 6 months since the date of communication and in accordance with the procedure established by the laws, and to provide the competent institutions free of charge with the data generated or processed by them. The duty of data storage includes also retention of data related to unsuccessful calls being generated or processed and stored (data of telephony) or registered (internet data) by the providers of public communications networks and (or) public electronic communications services in providing the appropriate services.

If the above-stated data are necessary for the entities of operational activities, the pre-trial investigation institutions, prosecutor, court or judge to prevent, investigate and detect criminal acts, the institutions authorized by the Government - on instruction from the entities of operational activities - the entities providing electronic communications networks and/or services must store such information for a longer period, but no longer than an additional six months. Such storage shall be paid for by state funds in accordance with the procedure established by the Government (Article 77(2) of the Law on Electronic Communications of the Republic of Lithuania).

The SDPI is responsible for the supervision of the implementation of provisions of Chapter 9 of the Law on Electronic Communications which also covers the provisions transposing the Directive 2006/24/EC.

2. **Secondary legislation**

2.1. SDPI granted as a responsible institution for collecting and providing the European Commission with statistics on the retention of data

The Resolution of the Government amending the Resolution of the Government ,,On Granting Authorisation for implementing the Law on Electronic Communications“ , No 788, was adopted on the 22nd July 2009. The SDPI was granted as a responsible institution for collecting and providing the European Commission with statistics on the retention of data generated or processed in

connection with the provision of publicly available electronic communications services or a public communications network according to the Article 10 of the Directive 2006/24/EC.

2.2. The procedures how law enforcement institutions provide electronic communications traffic data

The Resolution of the Government ,,On the Approval of Procedures of Providing Statistical Data Said in the Article 70 of the Law on Electronic Communications ", No 789, was adopted on the 22nd July 2009. This resolution describes the procedures how law enforcement institutions provide traffic data said in the Article 10 of the Directive 2006/24/EC to the SDPI and how the SDPI provides them to the European Commission.

2.3. Optimization of Functions of the Supervisory Institutions

The Resolution of the Government "On the Optimization of Functions of the Supervisory Institutions", No 511, was adopted on 4th May 2010. The aim of this Resolution is to optimize functions of the supervisory institutions, to lessen administrative burden to the private sector, to use more effectively assignations allocated to supervisory functions and to lessen risk of corruption. This resolution grants authorisation to the commission under the leadership by Vice-minister of Economy to help for Minister of Justice and the Minister of Economy to coordinate supervisory functions which are executed by supervisory bodies. There are 76 governmental institutions on the list which are grouped into 9 units by supervisory functions are to be coordinated. According to this Resolution the SDPI shall be designated in the Product safety group together with number of institutions empowered to supervise agriculture, fisheries, plants, buildings, metrology, gambling's, consumers' rights. The commission has right to analyse functions of institutions included in the list and to provide proposals regarding settled requirements of some fields of supervisory activity to the Minister of Justice and the Minister of Economy.

3. Major case law

3.1. Definition of personal data

The SDPI drew up record of administrative offence for a company that had collected personal data (names, surnames, addresses) from another company and used them to send offers to these people to sign up salvage contracts. The SDPI decided that there had not been any criteria for lawful processing of personal data.

The Kaunas district court stated that the definition of personal data provided in the paragraph 1 of the Article 2 of the LLPPD does not cover name, surname and address of natural person thus the LLPPD does not regulate legal protection of these data.

The decision of the Kaunas district court was appealed against at the Supreme Administrative Court of Lithuania. The Supreme Administrative Court stated that according to the paragraph 1 of the Article 2 of the LLPPD personal data shall mean any information relating to a natural person, the data subject, who is identified or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Also a

parallel definition is provided in the paragraph a) of the Article 2 of the Directive 95/46/EC. Considering these definitions, name, surname and address should be considered as personal data because a person can be identified according to his name, surname and address. The Supreme Administrative Court also noticed that The Court of Justice of the European Communities considers such data as personal data too (the Decision of 6th November 2003, case number C-101/2001).

3.2. Rights of data subjects

The SDPI received a complaint concerning collection of complainant's personal data from the Real Property Register. The SDPI decided that the criteria for lawful processing of personal data was the subparagraph 6 of the paragraph 1 of the Article 5 of the LLPPD (personal data may be processed if processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data are disclosed, unless such interests are overridden by interests of the data subject). Though the data controller (a bank) had to provide the complainant with the conditions for exercising the rights of data subjects, witch was not done, i. e., the data controller had not informed the complainant about collection of his personal data from the Real Property Register and had not informed the controller about his right to object to the processing of his personal data. Therefore the SDPI gave an instruction to the data controller to ensure that the subparagraphs 2 and 3 of the paragraph 2 of the Article 18 (the right to know (be informed) about the processing of his personal data) and the paragraph 1 of the Article 21 (the right to object against the processing of his personal data) of the LLPPD (version that was in force till 31st December 2008) would be implemented in the future.

The data controller appealed the instruction of the SDPI in a court, stating that the exception provided in the subparagraph 5 of the paragraph 2 of the Article 17 of the LLPPD (the data controller must provide the data subject with the conditions for exercising the rights laid down in this Article, with the exception of cases laid down in laws when it is necessary to ensure protection of the rights and freedoms of the data subject or other persons) had to be applied.

Vilnius District Administrative Court stated that the position of the SDPI accepting the personal data processing as legal, but stating that subparagraphs 2 and 3 of the paragraph 2 of the Article 18 of the LLPPD (version that was in force till 31st December 2008) were breached is illogical. The recognition of the SDPI that the data controller had legitimate interests to process personal data and these interests were not overridden by interests of the data subject does not suppose the obligation for the data controller to inform the data subject about his personal data processing. According to the subparagraph 5 of the paragraph 2 of the Article 17 of the LLPPD the data controller must provide the data subject with the conditions for exercising the rights laid down in this Article, with the exception of cases laid down in laws when it is necessary to ensure protection of the rights and freedoms of the data subject or other persons. Vilnius District Administrative Court concluded that the determined factual circumstances justifies the legitimate interest of the data controller and comply with the subparagraph 5 of the

paragraph 2 of the Article 17 of the Law on LPPD, thus the instruction of the SDPI was revoked.

The decision of Vilnius District Administrative Court was appealed against at the Supreme Administrative Court of Lithuania. The Supreme Administrative Court agreed with the argument of the SDPI that a decision that personal data are processed according to the Article 5 of the LLPPD (Criteria for lawful processing of personal data) does not presume that personal data processing was done according to all procedures provided in this law. Thus the decision of the court of the first instance that there is no a breach of the provisions regulating the rights of data subjects because the SDPI had decided that there had been a criteria for lawful processing of personal data was baseless.

According to the subparagraph 5 of the paragraph 2 of the Article 17 of the LLPPD the data controller must provide the data subject with the conditions for exercising the rights laid down in this Article, with the exception of cases laid down in laws when it is necessary to ensure protection of the rights and freedoms of the data subject or other persons. Therefore the right of the data controller not to provide the data subject with the conditions for exercising his rights should be situated with 2 conditions: this right of the data controller must be provided by a law (1) and these actions have to be necessary to ensure protection of the rights and freedoms of the data subject or other persons (2). In other words, if a data controller wants to apply this exception, only to try to ensure protection of the rights and freedoms of the appropriate subjects is not enough. Also this right of the data controller has to be provided in a certain legal act. The court of the first instance could not state that this exception had to be applied without indicating the other certain legal act because the subparagraph 5 of the paragraph 2 of the Article 17 of the LLPPD is a directive legal provision. The Supreme Administrative Court also stated that the data controller did not mention this exception to the SDPI while providing all the written explanations in the complaint investigation stage, thus the later arguments on the application of the exception could be considered as an intention to escape responsibility.

3.3. Video surveillance in the beauty salon

The SDPI received an anonymous complaint in which were stated what at the beauty salon in which amongst others are provided bikini zone depilation procedures are installed video surveillance cameras one of them is hidden and oriented to video survey whole body (even bikini zone) of the client, another – installed in the locker room. The SDPI decided that such video surveillance violates the paragraph 1 of Article 18 (processing of image data must be set down in a written data controller's document specifying the purpose and the extent of video surveillance, the retention period of video data, conditions of access to processed image data, conditions and procedure of destruction of these data and other requirements concerning legitimate processing of video data), paragraph 3 of Article 19 (it shall be prohibited to use video surveillance in premises where the data subject reasonably expects absolute protection of privacy and where such surveillance would undermine human dignity (e.g. toilets, changing-rooms, etc.)), subparagraph 2 of paragraph 1 and paragraph 3 of Article 20 (the data controller shall ensure that the data controller's contact

information (address or telephone number) and other requisites is clearly and properly provided before the entrance to the premises or territory in which video surveillance is used and if video surveillance is used in a work place and in the data controller's premises or territories in which the data controller's personnel work, the personnel must be notified of such processing of their image data in writing, according to the procedure laid down in Article 24(1) of the LLPPD) and the Article 31 Personal data may be processed by automatic means only when the data controller or his representative (pursuant to Article 1(3)(3) of the LLPPD) in accordance with the procedure established by the Government notifies the State Data Protection Inspectorate).

For the violations of the LLPPD the SDPI drew up record of administrative offence for an owner of the beauty salon. The Vilnius city first district court validated record of administrative offence and issued a fine to the owner of the beauty salon.

3.4. Spam

In year 2009 the number of complaints on processing of personal data for direct marketing purposes and the number of the issued records of administrative offences for that rose up to three times and constituted 25 percent of the all received complaints. Most of the complaints were about use of telephone number or email address for the direct marketing offers. Whoever the SDPI received a few complaints on the direct marketing offers to buy data bases of the telephone numbers and email addresses of the Lithuanian companies for the further use for the direct marketing. The SDPI immediately issued press release indicating that the use of such data bases and the creating and selling them is against the LLPPD and is punishable as administrative offence. Also the SDPI started investigations which at the moment are not finished yet.

4. Preventive activity

4.1. Video surveillance in gas stations

The chapter three of the LLPPD regulates video surveillance. The SDPI in pursue to find out how the protection of the right of data subjects is ensured while processing image data made inspections in 92 gas stations.

It was found that 33 of 92 gas stations do not use video surveillance. The breaches of the LLPPD were found in 57 gas stations.

According to the Article 31 of the LLPPD personal data may be processed by automatic means only when the data controller or his representative notifies the SDPI. The SDPI had been informed about video surveillance only by 2 inspected gas stations. Other 55 gas stations processed image data without informing the SDPI (11 gas stations of these 55 notified the SDPI while performing the inspections).

It was found that the gas stations do not ensure the right of data subjects' to know (be informed) about the processing of his personal data properly. 47 gas stations inform data subjects about video surveillance by special information signs, but do not provide the information about data controller and his requisites as it is required by the paragraph 1 of the Article 20 of the Law LLPPD. 27 gas stations provide the information about video surveillance in an inappropriate

distance, i. e., a data subject gets informed about video surveillance after he gets into the area of surveillance.
According to the paragraph 3 of the Article 20 of the LLPPD if video surveillance is used in a work place and in the data controller's premises or territories in which the data controller's personnel work, the personnel must be notified of such processing of their image data in writing, according to the procedure laid down in the paragraph 1 of the Article 24 of this Law. It was found that just 31 gas stations had notified their personnel in writing of processing of their image.
37 gas stations do implement the right of data subjects to have an access to his personal data and to be informed of how they are processed, but 15 of them ask data subjects to provide them with motivated and reasoned application, though the Article 25 of the LLPPD states that data subjects have the right to access if they provide data controller with personal identification document and a written application, i. e., without reasoning his application.
According to the paragraph 1 of the Article 18 of the LLPPD processing of image data must be set down in a written data controller's document specifying the purpose and the extent of video surveillance, the retention period of video data, conditions of access to processed image data, conditions and procedure of destruction of these data and other requirements concerning legitimate processing of video data. It was found that 25 gas stations had not had such document. 28 gas stations had had such documents, but they did not comply with the requirements of the paragraph 1 of the Article 18 of the LLPPD.
The inspected gas stations were provided with instructions regarding their breaches of the LLPPD.

4.2. Implementation of Directive 2006/24/CE.

The provisions of these directives have been transposed into Lithuanian legislation through the Law on Electronic Communications No. IX-2135 of the 15 April 2004. The amendments of the Law on Electronic Communications transposing the Directive 2006/24/EC entered into force since 16 March 2009. Pursuant to Article 15(3) of the Directive 2006/24/EC the Republic of Lithuania has declared that it will postpone the application thereof to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for the period provided for in Article 15(3).
The investigation was carried by written procedure and inspection in situ.

The Questionnaire was sent to four largest telecommunication companies working in Lithuania, which provide different types of telecom services (fixed telephony or/and mobile telephony and internet access), with EU / international dimension and also with largest market share. Each of these companies provide network and retail services using mainly their own network. One of them uses fixed network and provides fixed telephony and internet services. Others three companies use mobile network and provides mobile telephony and internet services. After analyzing the answers, the in situ inspections in these 4 telecommunication companies were performed.

All these operators retain traffic data for commercial and law enforcement purposes for 6 months. In a case if law enforcement authorities ask service providers to retain traffic data for more than 6 months traffic data are retained for not more than 6 months additionally. After expiry of the retention period, data are being deleted automatically. The systems are configured in the manner as to automatically perform data deletion. The anonymisation processes of traffic data are not carried out.

Traffic data for law enforcement purposes are stored together with all traffic data and are to be selected with special software when needed. Selection of the data for law enforcement purposes is maintained automatically but only authorized persons have access to the programs used for control and manual intervention. Three companies use proper users' Access Authorisation and Control. All users are provided with unique log in names and passwords. The authorizations of access to traffic data are provided only to those users that need traffic data to perform their duties.

All four operators indicated, that access is logged, although different data are recorded (e.g. access time, operations performed; the other enterprise records: when the CDR was taken from network's commuting station, when access is provided and to what data; the third enterprise registers user name, computer name or IP address, log in time, operation time and manner (viewed, copied, changed, printed, sent etc.), in some cases the output devices used are visible (if they are recognizable and information output is not directed to the monitor)); the company providing fixed telephony services is making records of IP address and date.

Three operators for sending of the responses to enforcement institutions use encryption (the company providing fixed telephony services uses encryption for data transmission channel between the user and database server by SSL protocol; two enterprises providing mobile telephony services reported that e-mails are encrypted by PGP key). One company providing mobile telephony services does not use data encryption.

The SDPI did not found out breaches of the Law on Electronic Communications, transposing the Directive 2006/24/EC and LLPPD. The protection measures, used by these four operators comply with the requirements indicated in General Requirements for Organisational and Technical Data Protection Measures, approved by Order of the Director of the State Data Protection Inspectorate, dated 12th of November 2008, No. 1T-71 (Official Gazette, 2008, No. 135-5298).

4.3. Publishing personal data on the internet

The LLPPD prohibit to process sensitive personal data except in case set out in Article 5 of paragraph 2. Municipal administrations published personal data of people who are on the waiting list for the accommodation in municipal residential premises (houses). The following data were collected and consolidated list which consist from a list of young families (family members should be under 35 year old), a list of families with care three or more children, list of orphans or deprived parent care persons and list of disabled persons or families if the family member is disabled person was published. The SDPI in pursue to find out how the protection of the right of data subjects is ensured while processing sensitive data

made inspections in 24 municipal administrations. Breaches of the LLPPD have been found in all 24 municipalities.
The inspected municipal administrations were provided with instructions as follows:

- to terminate publishing sensitive data in the internet;

- to implement appropriate organisational and technical measures delegated to data subject to obtain an information about processing of his/her data.

5. Public awareness

5.1. Conference "Privacy and Personal Data Protection in Lithuania"

The SDPI together with a joint stock company "Expozona" organized a conference "Personal Privacy and Data Protection in Lithuania" on the 26th November 2009. The purpose of this event was to introduce representatives of public and private sectors with privacy and data protection issues as much as it concerns privacy of employees, debt collection and video surveillance. The speakers participated not only from the SDPI, but also from companies working on supply of electricity (UAB "Eastern Distribution Networks"), pre-trial debt collection (UAB "Ekskomisarų biuras"), Administration of Vilnius City Municipality. 7 presentations were given on these topics:

- Shall we get back to "1984"? (privacy and publicity in the information society: tendencies and threats);

- An employee has the right to his privacy too;

- Personal data processing: how may it help to develop relations to customers?;

- Personal data processing and problems in pre-trial debt collection;

- Legal regulation of video surveillance;

- General requirements for the organisational and technical data protection measures;

- Video surveillance system in Vilnius city: now and in the future.

Also there were discussions and the members of the conference had possibility to ask questions, to express their opinion on the issues concerned.

5.2. Recommendations

a. The SDPI issued a Recommendation on "Privacy Protection in Video Surveillance Systems. Wireless Communications Technologies" on the 16th December 2009. It gives some recommendations how to protect privacy using CCTV, webcams and other video surveillance means, turns attention to risk and threats using these devices and describes possible organisational and technical data protection measures.

Full text (Lithuanian only) of this recommendation could be found at: http://www.ada.lt/images/cms/File/naujienu/IP%20kamera%20(Galutinis)%2020091216.doc

b. The SDPI issued a Recommendation on "Safe Data Transfer by https Protocol" on the 23rd December 2009. It covers such topics as installation of https protocol, activity principals of https protocol, types of SSL certificates. Full text (Lithuanian only) of this recommendation could be found at: http://www.ada.lt/images/cms/File/Inspekcijos%20rekomendacijos/SSL20091228.doc

5.3. PrivacyOS

The SDPI participated as a partner in the European scale project Privacy Open Space (PrivacyOS), which is aimed at bringing together industry, SMEs, government, academia and civil society to foster development of privacy infrastructures for Europe. Project is coordinated by the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), which is also the office of the Privacy Commissioner of the German State of Schleswig Holstein. The general objectives of PrivacyOS are to create a long-term collaboration in the thematic network and establish collective interfaces with other EU projects. Participants exchange research and best practices, as well as develop strategies and joint projects following four core policy goals: Awareness-rising, enabling privacy on the Web, fostering privacy-friendly Identity Management, and stipulating research.

Main topics in which Lithuania participated was E. Identification, E. Government, Healthcare and others. As a partner, the SDPI was designated with a budget of 14.400 € for the projects needs and the final dissemination of the project ideas and insights. Lithuania delivered presentations in 3 conferences of 4.

At the moment the project is at its ending phase – participants and the partners are preparing reports, sharing their insights and opinions on the last conference, which took place at 12-13th April in Oxford. The end of the project in Lithuania will be marked with conference on May 26th, during which Lithuanian companies in IT, modern technologies and public field will be presented with major insights, messages and topics from PrivacyOS project – Identity Management, RFID, e. mobility, security and privacy policy in information and communication technologies (ICT). Participation in the project to the SDPI was a great experience crowned with some very interesting insights that will definitely be applied in the SDPI's daily routine.

MACEDONIA

DIRECTORATE FOR PERSONAL DATA PROTECTION
REPORTING PERIOD
1st September 2008 – 31st August 2009

Personal Data Protection

Legal Framework

The Law on Amendments and Modifications to the Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" no.103/08) that entered into force in august 2008 strengthened the legal frame in the area of personal data protection in the Republic of Macedonia.

Furthermore, the Parliament of the Republic of Macedonia enacted the Law on ratification of the Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and cross - border data flow ("Official Gazette of the Republic of Macedonia" no.103/08). Republic of Macedonia transmitted the ratification instrument of the Additional Protocol to the Convention 108, with entry into force on 1st January 2009.

The Law on Amendments and Modification to the Law on Personal Data Protection stipulates that the articles referring to inspection will enter into force after the transitional period that expired on 28th of February 2009. With the implementation of the new inspection provisions, persons authorized for performing the inspection became inspectors for personal data protection, and are authorized to issue decisions in the cases when violation of the Law is determined. An appeal for administrative dispute to the Administrative Court could be applied against the inspector's decision. If the inspectors during the inspection determine a violation of the Law on Personal Data Protection, they take a legal action for alignment accordingly to the Law on Misdemeanors, but if an alignment is rejected, the inspector files a request for initiation of a misdemeanor procedure to the Misdemeanor Commissions of the Directorate. Accurate and short terms are determinate for the procedure that is taken during the inspection.

According the Amendment XX of the Constitution of the Republic of Macedonia and the Misdemeanor Law, Directorate for Personal Data Protection reach a status of the misdemeanor body that pass sentence upon misdemeanor sanction. This competence, until adopting the amendments and modifications to the Law on Personal Data Protection, was in the competence of the Macedonian courts but now is placed apart in a special chapter of the Law, dedicated solely to the Misdemeanors. For realization of this new competence, the Directorate for Personal Data Protection already constituted Misdemeanor Commission composed of three experienced lawyers, who will conduct and implement the misdemeanor procedure in practice. This will contribute with the increasing of citizen's confidence in the legal system in general, and especially in the protection of personal data protection, as well as improvement of privacy.

Besides the transfer of the jurisdiction for misdemeanor body that pass sentence upon misdemeanor sanction, adopting the amendments and modifications on the Law on Personal Data Protection will raise the fines, depending on the gravity of the infringement.
Now, they are divided into three groups: the fines for natural persons that are between €500 and €900, for responsible persons within legal entities the fines are from €700 up to €1200, and finally fines for legal entities are from €2000 up to €4000. In the Law there are fines for the processors: for natural persons fine is €600, for responsible persons within legal entities is €700 up and the fine for legal entities is from €2500.
According to the provisions of Law on Personal Data Protection, the following bylaws were adopted:

- Rulebook for the manner of the evidence files for the misdemeanors, the sanctions imposed and the decisions adopted, as well as for the manner of access to the information contained in the evidence files (Official Gazette of the Republic of Macedonia no.136/08)

- Rulebook for the manner of performance of inspections (Official Gazette of the Republic of Macedonia no.143/08 and 38/09)

- Rulebook for the manner of the form and content of the official identity card, as well as the manner of issuance and revocation (Official Gazette of the Republic of Macedonia no.143/08)

- Rulebook for the form and the notification form as well as the manner of notification in the Central Register of personal data collections (Official Gazette of the Republic of Macedonia no.155/08)

- Rulebook on the technical and organizational measures on provision of secrecy and personal data protection (Official Gazette of the Republic of Macedonia no.38/09)

The Directorate for Personal Data Protection has filed Annual Report about the working period from 1st of January to 31st of December 2008. This Annual Report represents an act for achievements and realized program activities in 2008, but also a perspectives and recommendations for 2009. On 30th April the Assembly of Republic of Macedonia has adopted the Directorate's Annual Report.

Implementation of the Law on Personal Data Protection

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

Inspection of legality of the activities for processing and protection of personal data over the controllers and processors i.e. the holders of personal data collections is one of the key competences of the Directorate.
Priority areas for inspection in this period were: education, health, social security, telecommunications, property insurance and marketing. Inspections were

performed in state bodies, local self government, NGO's, political parties, public enterprises and other legal persons with different activities.
During the period of September 2008 till August 2009 the Directorate has been performing inspections, as evident from the table below.

Areas	Performed supervisions
Banking	4
Consulting services	1
Education	13
Health	7
Local self government	6
Natural persons	2
NGO's	6
Pharmacy	3
Political parties	1
Post services	1
Property insurance	5
Security and Detective Agencies	1
Social protection	3
State bodies	5
Telecommunication	5
Tourism	2
Trade	6
Waste collection service	3
Water supply	1
Total:	**75**

During reporting period, citizens especially were submitting initiatives for performing inspection on personal data processing over the video surveillance, personal data processing for purposes of direct marketing, without being asked for previous consent from the controllers, collecting of the personal identification number of the citizens without legal base and retaining of the personal card of the citizens while entering official premises of certain controllers.
Inspection performed by the inspectors of the Directorate may be regular, irregular and control.
Regarding the reporting period the fallowing inspections have been performed:

Type of inspection	Performed supervisions
Regular	**37**
Irregular	**37**
Control	**1**

Total:	**75**

Also, with the Annual program for performing inspection of the Directorate for the third quartile are projected/planed regular inspections at the law enforcement bodies. In that context meetings were completed with certain representatives of the Ministry of Internal Affairs and Ministry of Defense, Office for Preventing Money Laundering and Financing terrorism and Customs Administration of the Republic of Macedonia. These meetings were held aiming the compliment of the work of the named state bodies with the Law on Personal Data Protection.
Performing the irregular inspections authorized persons from the Directorate in one case determined a misdemeanor according to the Law on Personal Data Protection at a controller of the banking area. A fine of 2000 euro was imposed, and the procedure ended with alignment.
During the reporting period against two decisions issued by the Directorate for Personal Data Protection was initiated administrative dispute, for which the procedure at the Administrative court of the Republic of Macedonia is still running.

- ***Providing expert opinions***

The Directorate during the reporting period has been providing opinions on protection of personal data as one of the fundamental rights and freedoms of natural persons. The majority of the opinions were for privacy policy on Internet, documentation for technical and organizational measures which provides secrecy and protection of the processing of the personal data in accordance to the nature of the data that are processed and the risk during their procession prepared by the controllers, transfer of personal data to other countries, permission about processing personal data, questions by natural or legal persons, particularly related on abusing the personal data on Internet. Also, the Directorate has issued permission about processing biometric data in the banking sector.

The Directorate has issued 15 opinions on draft laws and 9 opinions on international agreements in accordance with the competencies stipulated in the Law on Personal Data Protection.
The Directorate has adopted the Rulebook on the technical and organizational measures on provision of secrecy and personal data protection. According to the article 10 of above mention Rulebook, the controllers who processes personal data need to apply technical and organizational measures, which provide secrecy and protection of the processing of the personal data, in accordance to the nature of the data that are processed and the risk during their procession. The technical and organizational measures are classified on three levels: basic, medium and high. The Directorate issues opinions for the compliance of the documentation for technical and organizational measures prepared by the controllers with the provisions of the Law on Personal Data Protections, bylaws and data protection principles, acting according to the principle ex ante.

Area	Provided opinions
Pension and disability insurance	6
Banking	15
Finance	4
Telecommunications	10
Direct marketing	11
Health	12
Law firms	19
State bodies	117
Natural persons	94
International	31
Political Parties	1
Consultations provided by phone	119
Internet	15
Public enterprises	3
Tourism	3
Media	3
Incompetence	2
Chambers of commerce	4
Education	11
Legal persons	15
Associations	1
Security	1
Judiciary	1
NGO	1
Social security	1
Post	3
Total	503

Providing reprimands

The Directorate has issued 29 reprimands for consequently enforcement on the provisions and principles for data protection from the controllers and processors of the personal data collection. Most of the reprimands were given to the state bodies that according to the provisions of Law on Personal Data Protection and data protection principles collected and processed personal data excessive in relation to the purposes for which they are collected and processed, such as Ministry of Justice and Ministry of Education and Science.

Also, the Directorate for Personal Data Protection has taken measures and has given reprimand about public announcement of the judicial decisions on the web

site of the Primary Court, Kavadarci. Namely, in the judicial decisions that were published by the court personal data were not anonym.

The Directorate also issued Recommendations for the citizens and Internet providers for use of social network sites, in particular how to protect their privacy and personal data when they are online. The Recommendations are published online, on the web site of the Directorate.

Area	Provided reprimands
Direct marketing	1
State bodies	10
Natural persons	7
International	1
Internet	3
Media	1
NGO sector	1
Political parties	1
Pension and disability insurance	1
Education	2
Legal persons	1
Sport	1
Total	30

- ***Complaints handling and requests by citizens***

With the Law on Amendments and Modifications to the Law on Personal Data Protection, the procedure for injuries of the right of personal data protection requests was simplified, on the way that Committee within Directorate for complaints handling as first instance was declined and decision making procedure, as first instance, by the director of the Directorate was inducted. Against director's decision an appeal can be submitted for actuation of administrative procedure in the front of Administrative Court of the Republic of Macedonia, in 15 days from the day of receiving the decision.

REQUESTS	SUBMITTED	ESTABLISH VIOLATION	REJECTION	IN PROCESS	MISDEMEANOUR REQUSETS
Direct marketing	5	2	3	/	/
Judiciary	2	1	1	/	/
NGO	14	8	4	2	/

State bodies	**14**	**10**	**3**	**1**	**4**
Telecommunications	**18**	**7**	**5**	**6**	**/**
Private sector	**2**	**/**	**2**	**/**	**/**
Insurance	**2**	**1**	**1**	**/**	**/**
Internet	**16**	**4**	**11**	**1**	**1**
Banks	**2**	**2**	**/**	**/**	**/**
Political parties	**3**	**1**	**2**	**/**	**/**
Natural persons	**4**	**/**	**/**	**4**	**/**
Mediums	**5**	**2**	**3**	**/**	**/**
TOTAL:	**82**	**36**	**32**	**14**	**5**

- ***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.

Media	**Appearances**
Printed media	**106**
TV	**66**
Radio	**15**
Total	**187**

- ***Events and projects***

European Commission and the TAIEX Instrument in cooperation with the Directorate for Personal Data Protection organized **"Seminar for Personal Data Protection in the Framework of Police and Judicial Co-operation in Criminal Matters"** on 25-26 September 2008, attended by ministry officials, civil servants, judges and public prosecutors in the area of police and judicial cooperation in criminal matters. The seminar gave a detailed insight into international and European legislative instruments in the area of data protection. Special attention

was paid to the data protection requirements that need to be met in order to exchange information within the Schengen Information System and to prepare for a potential Schengen evaluation, as well as exchanges with the EU's agencies for police and judicial cooperation in criminal matters, i.e. Europol and EUROJUST.

Seminar **"Personal Data Protection in the Election Campaign"** was held in Skopje on 27 September 2008 for the all political parties. The aim of the seminar was education for the processing, usage and protection of personal data protection of the most important participants in the election process – political parties.
Public debate **"Is it really safe with cameras"** was held on 10 October 2008 on the Law Faculty, Ss Cyril and Methodius University. The goal of the debate was human right promotion and raising the awareness about the risks for privacy coming from information technology development.
The project **"Children's Rights on the Internet – Safe and Protected"** is project established in cooperation with the Metamorphosis Foundation, supported by the European Union in which the Directorate participates. The aim of the project was arising of the awareness for existing issues on the internet, if there is no rightful usage and protection.
On the occasion of the European Data Protection Day, 28 January in 2009 the Directorate prepared presentation of **"Guidelines for personal data protection of the students".** Considering the fact that young population, especially the students in the public education system, is one of the most important target groups, this year the Directorate decided to dedicate the European Data Protection Day to them.
On the occasion of the celebration of the Safer Internet Day 2009, the EU Info Centre in Skopje organized a Panel discussion entitled **"How to make the Internet a safer place".** The aim of this panel was raising awareness and opening debate about the issue of safe and responsible use of new technologies, particularly the Internet.
The Directorate provided presentation about the aspects of personal data protection on internet.
Trainings for **the right on free access to information** - the responsible person for free access of information within the Directorate is included in this project as a trainer.
Directorate performed two trainings as expert assistance to interested controllers during April 2009. The first one was held for the **Coalition for protection and promotion of sexual and health rights of marginalized communities** and the second one was for the **students of law on the American College in Skopje.**

- ***International cooperation activities***

Membership in conferences and other networks

The Directorate is a member of the **International Conference for Personal Data Protection, Spring Conference of the European Data Protection Authorities, Conference of Data Protection Authorities from Central and Eastern Europe, Consultative Committee (T-PD) for Personal Data Protection of the Council of Europe** and has 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 the EU countries.

Eurojust

During April 2008, Republic of Macedonia and EUROJUST began negotiations for signing a Collaboration Agreement in purpose of strengthening the effectiveness of institutions for investigation and pursuit of serious forms of cross border and organized criminal. The negotiations results with signed Collaboration Agreement between Republic of Macedonia and EUROJUST, on 28th of November 2008 ("Official Gazette of the Republic of Macedonia" no.51/09).

Europol

Directorate for Personal Data Protection has an active participation in preparation of Republic of Macedonia for signing an Operative Collaboration Agreement with EUROPOL. In this direction, in December 2008 a study visit was realized in the Directorate for Personal Data Protection by the EUROPOL experts for comprehension in the administrative practice during data exchange. EUROPOL has prepared a Report with highly positive evaluation of the condition in this area. EUROPOL stipulates that there was complete accordance with the European legislation and successful and practical implementation of the Law for Personal Data Protection.

Visa liberalization

Directorate has continuously worked on realization of the commitments that came out from the European Union Directions for visa liberalization by filing monthly reports from the area of personal data protection. This practices pursuit in 2009. European Commission in its Report for visa liberalization points that the Directorate for Personal Data Protection is young, modern and dynamic institution, which successfully cooperates with police and judicial sector and accomplish active international cooperation in this area.

Other issues of interest

- **Establishment of International Law Enforcement Co-ordination Units (ILECU'S) –** the Directorate is included in this CARDS Regional Action Program. The ILECUs are to be created as national coordination points for the exchange of information in international investigations and of facilitating contact on strategic and operational level. It is essential that these units are integrated in a national criminal intelligences model in each country and supported by proper data protection and confidentiality regimes. In role of project's support, a Memorandum of Understanding was prepared by member states representatives, where Directorate for Personal Data Protection had a proactive participation. As following stage in the progress of the ILECUs was creating of

the Action Plan and defining of priorities and future activities for further realization. Directorate for Personal Data Protection is included in all phases of the work of the ILECUs, as supervisory authority regarding protection of citizens' personal data and induction of the personal data provisions.

- The Directorate is participating in the **Project for Establishment of a National Intelligence Data Base.** Directorate for Personal Data Protection as national supervisory authority is participating in the Project for Establishment of a National Intelligence Data Base. The aim of this project is preparing a Law on National Intelligence Data Base as legal instrument for establishing and functioning of the National Intelligence Data Base, processing of the data within base, safety of the data within base, usage of the base in purpose of cooperation with foreign entities and supervisory over Base's functioning. As precursor of establishing of the NID a Feasibility Study was prepared in cooperation with other law enforcement authorities in Republic of Macedonia. In the time of preparing of the mentioned Feasibility Study, Directorate for Personal Data Protection was constantly amending the "corpus" of the Study with provisions for protection of the personal data in purpose of avoiding the excessive procession of citizen's personal data trough this Base.

- **Police Cooperation Convention for Southeast Europe (PCC SEE)** – the Directorate is actively included in all activities connected with the PCC SEE. The aim of these Programs and Projects is international implementation of the Laws that refer to the combat of organized crime through efficient transfer of data, excellent organization and implementation of international standards.

- **Schengen Action Plan -** The Directorate continuously assist the Ministry of Interior in the process of preparation of the Schengen Action Plan.

- **Data exchange Protocol between Database and Information System –** the Directorate is actively included in all activities connected with this Project that aims to increase the efficiency of the work of public administration.

- **Integrated database for aliens, covering asylum, migration and visa** – the Directorate is included in the Project for establishment of integrated database for aliens, covering asylum, migration and visa that aims to introduce a database which will contain all necessary personal data for aliens that are needed for asylum, migration and visa.

Capacity Building

At this moment Directorate has 21 employments and two assistants on the Project for approximation of the legislation – Law Program, Foundation Institute Open Society – Macedonia. According to the NPAA, by the end of 2010, the Directorate is to consist of approximately 40 employees.

MALTA

INFORMATION ON THE 2010 DATA PROTECTION DAY AND ON MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD SINCE THE 25TH MEETING OF THE T-PD

DATA PROTECTION DAY 2010

On 28th January 2010 the Office of the Data Protection Commissioner celebrated the 4th Data Protection Day of the Council of Europe. As it is the idea of this Office that data protection awareness should be particularly instilled in the younger generation, in order to mark this day the Office embarked on a data protection awareness campaign for children. This consisted in distributing posters and stationery items conveying a data protection message to school children. This message centred around the fact that one should be very careful when providing personal data on the internet in particular when logged onto social networking sites.
In addition to the above, the Office also included information concerning data protection day on its Portal, for the benefit of the public at large.

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD SINCE THE 25TH MEETING OF THE T-PD

Since the 25th T-PD meeting, the Office of the Data Protection Commissioner continued addressing the considerable amount of complaints of a data protection nature, it received. The majority of these were sent by private citizens alleging that their privacy was being undermined due to, amongst others, the installation of CCTV cameras, unsolicited communications and photos or videos posted on social networking sites without the consent of the data subject concerned. A number of these complaints led to inspections carried out by this Office in order to ascertain the veracity of the facts being alleged.
Throughout this period the Office also received a number of queries concerning the interpretation of the Data Protection Act and its subsidiary legislation, the obligations imposed on entities which process personal data and the rights of data subjects.
The Office organised out of his own motion and also attended upon invitation, a number of meetings with various sectors, national authorities, constituted bodies and entities in order to give its interpretation and discuss the applicability of data protection legislation. In addition, a number of presentations were delivered on the subject of data protection in general with the main aim of increasing awareness. Representatives of the Office also took part in European and Internal fora on data protection.
The Data Protection Commissioner, Mr Joseph Ebejer, contributed to the workings of the Article 29 Working Party, of which he is an active member.

NETHERLANDS

[Concept Pauline Hoefer 25-5-2010 met opm. Dominique Hagenauw verwerkt]

12th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and third countries covering the year 2009

Input of the Netherlands

Implementation of Directives 95/46/EC and 2002/58/EC

Directive 95/46/EC was transposed into national law, the *Wet bescherming persoonsgegevens* (Wbp) [Dutch Data Protection Act]. This was done by an act of 6 July 2000[2] which entered into force on 1 September 2001, replacing the old data protection law, the *Wet persoonsregistraties* (Wpr), which dated from 28 December 1988.

Directive 2002/58/EC has been transposed into Dutch law mainly by the changed *Telecommunicatiewet* (Telecommunications Act) that entered into force on 19 May 2004[3]. Other legislation transposing parts of this directive are amongst others the *Wet op de Economische Delicten* (Act on Economic Offences), that implements article 13(4) of Directive 2002/58/EC.

Main themes

The Dutch Data Protection Act is currently subject to evaluation. In view of the possible revision of the Act the Dutch DPA [College bescherming persoonsgegevens (CBP)] has stressed the importance of strengthening the position of data subjects. They should easily have access to information about why their personal data are being processed, which measures preventing illegal use of those data have been taken and how they can exercise their rights. Apart from that, easily accessible complaints procedures should be developed/introduced, as well as the possibility of class actions.

As to the position of the controller, a shift is taking place from ex ante supervision to ex post supervision. Controllers should invest more in complying with the law and should have to pay for non compliance. The Dutch DPA propagates more transparency, a requirement to report data leaks and the use of privacy by design.

Thirdly, the position of the supervisory authority itself should be strengthened.

[2] Act of 6 July 2000, concerning regulations regarding the protection of personal data (*Wet bescherming persoonsgegevens*), Bulletin of Acts, Orders and Decrees 2000 302. An unofficial translation of the act is available at the website of the Dutch Data Protection Authority, www.dutchDPA.nl or www.cbpweb.nl.

[3] Act dated 19 October 1998, concerning regulations regarding telecommunication (Telecommunications Act), Bulletin of Acts, Orders and Decrees 2004, 189.

Next to its work as an advisor of the government concerning new legislation effecting privacy, the Dutch DPA in its supervisory role has opted to give priority to enforcement in the conviction that by doing so, it is able to make the most effective contribution to the promotion of compliance with the *Wet bescherming persoonsgegevens* (Wbp) [Dutch Data Protection Act]. For the purpose of establishing the priorities for 2009, a risk analysis was made of the processing of personal data in different sectors of society. The Dutch DPA subsequently selected cases which contained indications of serious violations of the law, which were structural in nature, affected many citizens, and against which the Dutch DPA had the power to take action. The Dutch DPA also kept its eyes open to topical events in the course of the year. The investigations and interventions carried out by the Dutch DPA (108 in 2009) did not only achieve results with individual controllers, but also appeared to have indirect effects.
The thematic 'guidelines' for 2009 entailed the obligation to provide information on and transparency about the transfer of personal data to third parties.

Major issues

The internet

After an investigation into the Internet company Advance the Dutch DPA concluded that the company had violated the law by collecting sensitive data of people using Internet platforms and subsequently selling their profiled personal data to third parties without having informed the persons concerned about this clearly and fully. At the time, approximately 2.2 million people participated at Advance's Internet sites. Advance offered them the possibility to complete a test, for instance, to find out 'your real age'. The investigation revealed that Advance had collected and processed, among other things, medical data, whereas this activity is in principle subject to a statutory prohibition. Advance had not informed the persons concerned about the use of their data in accordance with statutory requirements.
A site used to assess teachers by their pupils caused serious damage to the privacy of the teachers concerned. Following investigation by the Dutch DPA the site was adapted and shielded from search engines.
The Dutch DPA also investigated two sites aimed at young people. The social networksite www.zikle.nl was required to inform its users adequately about the goals for which personal data were collected and processed, to apply security measures and to shield pages containing personal profiles. Www.jiggy.nl used a game to entice users to hand over email addresses of other people for direct marketing purposes. After investigation, the proprietor of the website removed the game.

Financial data

After the introduction of the instrument of an Advisory Letter in 2008, the Dutch DPA drew up its first advisory letter in 2009 at the request of the Stichting Landelijk Informatiesysteem Schulden (LIS), [National Information System of Debts], which was followed by a second advisory letter in response to a new draft of the LIS. Tests conducted by the Dutch DPA revealed that neither of the drafts

complied with the statutory requirements. With respect to the second draft, the Dutch DPA concluded that the draft far exceeded the original purpose of the draft, i.e. the registration of overdue debts to avoid problematic debts. This may result in the fact that a substantial group of people will be registered who do not belong in the register but who will be confronted with the negative consequences of being reputed as a problematic debtor.
A bank passed on young clients' account numbers and addresses to a charity, without informing the clients or asking their consent. Following a complaint the Dutch DPA investigated the matter, which led to adaptation by the bank of its routine.
In 2009 the Dutch Finance Minister followed the DPA's advice on legislative proposals for the establishment of a pension registration. The idea is that each citizen can check his or her retirement pay rights on line. As these data will undoubtedly attract other parties, the Dutch DPA pointed out the necessity for tight security measures.

Medical data

On the basis of investigations at two current regional electronic patient records systems (reprs), the Dutch DPA established that the Wbp had been violated. The Dutch DPA initiated compliance procedures against both reprs. These procedures resulted in the fact that one of the two reprs ceased the unlawfulness established, by, among other things, informing all patients personally about the inclusion of their data in the reprs.
Proposed legislation on electronic patient records continued to cause concern. Critical advice of the Dutch DPA on the initial legislative proposal in 2007 led to adaptation of the draft. Amendments by the House of Representatives however made it possible in some cases for health care insurers to have access to patient records. The Dutch DPA advised the minister to delete this exception to the general prohibition. The Minister has indicated he will follow this advice.
Another cause for concern regards information security in hospitals. Investigations carried out by the Dutch DPA and the Inspectie voor de Gezondheidszorg (IGZ) [Netherlands Healthcare Inspectorate] in 2007 and 2008 revealed that none of the twenty hospitals investigated complied with the standard for information security. In 2009, the Dutch DPA imposed orders subject to a penalty for non-compliance on four hospitals that still had not properly organised this aspect.
Investigation into the procedures of a number of occupational health and safety services resulted in the conclusion that at least one service – Tredin – acted systematically in violation of the law by providing medical data of sick employees to their employers whereas these data were subject to medical confidentiality. The Dutch DPA imposed an order subject to a penalty for non-compliance on this health and safety service in 2009. The health and safety service subsequently ceased the violations within the compliance period set. The investigation into three other occupational health and safety services has been continued.

Other activities in the private sector

We might seem to get used to it, but supervision by camera remains a far-

reaching means, about which the Dutch DPA receives a lot of questions from citizens. The Dutch DPA investigated the use of camera surveillance in an industrial estate. The findings were generally positive for the company that is responsible for the surveillance. The company promised to change the rules on inspection in order to make them consistent with the requirements of the Wbp. Because it isn't always clear if private companies or government bodies are responsible for camera supervision, the Dutch DPA has decided to develop new Guidelines on the subject.
A lot of buzz was generated by the proposed introduction of the so-called 'smart' electricity meter, which can provide a very detailed picture of someone's household and thus also of the periods people aren't at home. Consumers should be allowed to make informed choices regarding the frequency and amount of information that can be collected. The draft bill has been amended following the Dutch DPA's advice to the Minister.

Young persons

The digital processing of personal data in general and by the government in particular explicitly demands safeguards. This applies all the more where information relates to children and young persons.
In 2008, the Dutch DPA issued highly critical advice on the draft legislative proposal that would result in the creation of a Verwijsindex Risicojongeren [reference index for young persons at risk]. Criticism focused particularly on the object of the reference index, which is insufficiently concrete and, combined with its unclear criteria for the registration of a young person by his or her care provider, entails an almost inevitable risk of arbitrariness. Although the legislative proposal submitted on 6 February 2009 responds to the criticism raised by the Dutch DPA – amongst others – in several areas, the essence unfortunately remained the same. In 2009 the Dutch DPA was asked for advice on a number of executory measures the new bill entails and again, warned for arbitrariness.
Primary schools issue educational reports on their pupils to secondary schools. The Dutch DPA has investigated compliance with the information obligation to the parents of children in this situation. This is vital for the possibility of correcting the report, which can have a protracted negative effect on children if it contains incorrect or outdated information. More than half of the schools that were investigated did not record if the parents were informed or not. Following the investigation the Dutch DPA issued Guidelines for primary schools on the subject.

Police and the judicial authorities

Safeguarding the correct and transparent use of personal data is vital in light of the
increased powers that police and the judicial authorities have in relation to the processing of personal data. In 2007/2008, the Dutch DPA investigated the internal exchange of personal data within the police forces via the police information desk. By far the majority of police regions were found to be completely unequipped for compliance with the requirements of the Wet politiegegevens [Police Data Act], which became effective on 1 January 2008. In 2009 a follow up investigation in three regional police forces showed that, setting

aside differences, none of the forces complied fully with the requirements for authorization and monitoring.
Intelligence services can compare their information directly with police records. In an advice regarding proposed legislation on this independent form of consult of police databases the Dutch DPA has asked the government to make clear why this large scale consultation is necessary.
In 2009, the Dutch DPA developed guidelines for the purpose of automated number plate recognition (ANPR) by the police. In these guidelines, the Dutch DPA explains which interpretation of the statutory standards it maintains as a supervisory authority in exercising its powers. Later on in the same year, the Dutch DPA conducted investigations into the application of ANPR by two police forces and concluded that both police forces knowingly acted in violation of the *Wet politiegegevens* (Wpg) [Dutch Police Data Act] by processing hits and no-hits 120 or 10 days, respectively. A no-hit means that a scanned number plate does not occur in the reference file and that this number plate is consequently not sought by the police. The registration of this number plate must be destroyed immediately. In response to the publication of the final investigation findings, both forces announced at the beginning of 2010 that they would cease the unlawfulness.
Passengers who want to participate in a system allowing for automated border passage, for example by means of an iris scan or fingerprints, have to be screened beforehand. The Dutch DPA has asked the Minister of Justice to make clear which starting points will be used in these background investigations.

POLAND

Information on recent developments at national level in the data protection field

Revision of the Telecommunications Act

On July 6, 2009 the Act of April 24, 2009 on the amendment of the Telecommunications Law entered into force. The amendments were, among others, new provisions on data retention, adapting the national legislation to the requirements set forth in the Directive 2006/24/EC it imposed the public telecommunications network operators and providers of publicly available telecommunications services, many additional responsibilities, like the obligation to retain traffic data for a period of 24 months from time of the call, and after that time to destroy such data, except for those retained under other provisions of law. The above-mentioned obligations should be implemented in a way which does not result in the disclosure of the telecommunication transfer. Introduced amendment also requires the entrepreneurs to ensure the security of personal data through appropriate technical and organizational measures and also through ensuring access to this data only to authorized staff.

The draft of the Act on the amendment of the Act on the access to public information, which provides the recognition of the data concerning the health condition of the persons holding the posts of the President and Prime Minister as public information. Inspector General, clearly expressing his negative attitude towards the provisions of the draft pointed out that the existing provisions of the Polish Constitution, the Act on the Protection of Personal Data and Directive 95/46/EC are all recommending the legislator to keep far-reaching moderation in terms of introducing the solutions that might result in publicizing data on health status - as called. of "sensitive" - even if it were to apply to holders of the highest public positions in Poland. He stressed that although the right to privacy and right to the protection of personal data of public office holders is much narrower than the "ordinary citizens" there is no legal basis that would allow to assume that these rights shall not apply at all. The data protection authority highlighted that this position was reflected also in the Declaration on the freedom of political debate in the media of the Committee of Ministers of the Council of Europe of 12 February 2004.

Because of the firm position of the Inspector General the above-mentioned draft did not enter into force, and any further attempts of its introduction will meet with fierce reaction of the DPA.

The new Regulation by the Minister of Internal Affairs and Administration on **specimen of a notification of a data filing system to registration** by the Inspector General for Personal Data Protection entered into force on February 10 2009. In the new specimen notification, elaborated on the initiative of GIODO, simplifications were made and the principal responsibilities of data controller with

regard to data safeguarding were enumerated. The introduction of the new specimen resulted in a decrease in the number of wrongly filled notifications.

Major case law

During the reporting period the Inspector General has considered several cases relating to the activities of the Credit Information Bureaus. The Supreme Administrative Court in its jurisdiction has reaffirmed the position of the Inspector General on several cases. One of the most important cases was that the Bureaus, as data controllers were charging their clients for performing access to their personal information. This practice has met with strong opposition of the Inspector General. According to Polish provisions the data subject has a right to access information once every six months and the access should be free. With reference to the above such approach has been confirmed in a decision issued by the Supreme Administrative Court on 30 July 2009

The Inspector General also dealt with the problems of acquisition and processing biometric data for purposes of supervision of working time. The Inspector General stood on the position that such action is too far-interference in the privacy of the data subject. In such cases there is always a big risk of the violation of privacy, and there is a need to choose other, less intrusive methods. This position has been confirmed by the Supreme Administrative Court, which, in its ruling of 1 December 2009 held that in assessing the desirability of obtaining, with the consent of the employee, of their biometric data for the verification of working time it should be noted that that the major prerequisites of processing in such cases shall be the principals of proportionality and legality. It means that the risk of breaking of freedoms and fundamental rights must be proportional to the purposes for which such data are processed. Since the principle of proportionality expressed in the Act on personal data protection is a primary criterion for decisions related to the processing of biometric data, it should be noted that the use of such data to control the working time is disproportionate to the intended purpose of their processing. The Court stood on the position that gathering of biometric data in such cases would have to be seen as the excessive intrusion into privacy and thereby confirming the position of Inspector General.

During the reporting period Inspector General also investigated the question of the admissibility of the processing of personal data in the backup copies created by the banks after the removal of data from the data filing system, in the absence of legal grounds for further processing. Such a situation may arise when after the negative consideration of the credit application the bank removes the personal data of the applicant from the filing system due to the fact that the legal basis resulting from the data protection Act has expired. (processing of data necessary to undertake activities needed for the conclusion of the contract). Then the processing of data in backup copies, when the data is no longer in the filing system, is contrary to the purpose for which such copies are made (archival purposes related to ensuring the operational safety of the bank). The above position of Inspector General was confirmed in the judgment Regional Administrative Court in Warsaw of 16 January 2008, and then the Supreme Administrative Court dismissed the cassation complaint on 3 July 2009.

Major specific issues

In June 2009 GIODO controlled the processing of personal data in IT systems of the Public Transport Authority of Warsaw (ZTM) pursuant to press articles on ZTM gathering information related to ZTM recording places and times of public transport travel (in particular in the Warsaw underground, where at each entrance the passengers need to press an electronic card encoding the ticket to the gate in order to open it. The inspection confirmed the existence of the problems pointed out by the press and other irregularities related to excessive data processing in the scope inadequate to the purpose. GIODO informed ZTM of the irregularities discovered in the course of the inspection and demanded their remedy. At present, the Inspector General is performing inspections in other cities in order to verify the scope of data processing carried out by other public transport companies which opted for ticketing systems similar to the one used by ZTM.

The ZTM control case described above was the cause of a broader audit conducted by the Inspector General in the other carriers.

Social networks.

In the first and second quarter of the year the Inspector General conducted a series of checks in social networking sites. In the course of the inspections it was established that, as a rule, data controller is the provider of the website, however, in some cases the active users create specific sub pages, seize the initiative concerning the purpose of actions and the “mission” of other users, who gather around them. The irregularity discovered the most often during the inspections in such entities was inadequate protection of data collected on users’ profiles. The process of logging in and editing the profiles was often weakly safeguarded (too short passwords, transmission of unsecured data). Organizational faults comprised shortcomings in fulfilling the obligation to inform, lack of clear information on the possibility of reporting abuse and imprecise regulations. As a result of the actions undertaken by the Inspector General, in cooperation with the administrator of “Nasza Klasa” (Our Classmate) , there was a separate tab created on the website of the portal, allowing to read about the data protection issues, privacy threats, and introduced the functionality to allow you to set the security level of user data.

In 2009, the Inspector General conducted an inspection on the entities who are entitled to direct access to the National Information System which allows to make an entry to the SIS and to access SIS data. Primarily the courts were the subject of control. The audits found many irregularities, such as lack of proper documentation (e.g. lack of security policy) and that the unauthorized persons with no adequate training have the access to personal data. After the inspection and irregularities are found in the Inspector General asked the Minister of Justice to address the matter and correct irregularities in particular those related to the implementation of access to the Schengen Information System.

The Inspector General is continuing educational initiatives aimed at raising awareness among citizens about their right to data protection and privacy. Another educational project is a pilot program aimed at junior high schools, "your data - your business - Effective protection of personal data. Educational initiative aimed at students and teachers. " The purpose of an educational initiative aimed

at teachers and junior high school students to increase their knowledge of data protection and the right of everyone to privacy protection. The program involves cooperation on the basis of partnership between the self-government training centers for teachers and the General Inspector for Personal Data Protection. Pilot consists of two stages. In phase I, it was founded to train teachers, while phase II is the inclusion of the data protection matters into the teaching programs. The schools involved in the program will be provided with the outlines and materials for students and teachers prepared by Inspector General, as well as there will be evaluation report of activities undertaken and the project of the nationwide educational program.

On 27 January 2009, as a part of the 4th Data Protection Day the Inspector General signed an agreement with the Polish Bank Association entitled „Best practice of personal data processing in banks – from the perspective of practitioners" for the benefit of raising standards of personal data protection and the right to privacy in the banking activity. This agreement is meant to help to create the code of best practice in data protection for the whole banking sector.

The Inspector General for Personal Data Protection in cooperation with the Episcopate of Poland developed the "Guidelines on Personal Data Protection in the Activity of the Catholic Church in Poland".

The Guidelines clear the principles of proper safeguarding of personal data and are aimed to help protect personal data in the activities undertaken by the Church besides the fact that the controlling powers of the Inspector General are very much limited as far as the operation of the Church is concerned.

PORTUGAL

La liste des normes législatives du Portugal concernant la protection des données à caractère personnel en 2009 :
- Décret-Réglementaire 3/2009 du 3 février – réglemente l'article 1er de la loi 19/2008 du 21 avril ayant pour objectif la création dans le cadre du Ministère de la Justice d'une base de données de procurations;
- Acte réglementaire (Portaria) 270/2009 du 17 mars – détermine l'information ADN à intégrer dans le fichier de profils ADN existant dans la base de données de profils ADN à des fins d'identification civile et criminelle ;
- Loi 34/2009 du 14 juillet – établit le régime juridique applicable au traitement de données référant
au système judiciaire et procède à là deuxième altération à la Loi n. 32/2004 du 22 juillet, qui établit le statut de l'administrateur de la faillite;
- Loi 74/2009 du 12 Août – approuve le régime applicable à l'échange de données et informations de nature criminelle entre les autorités des États Membres de l'Union Européenne en transposant pour l'ordre juridique interne la Décision-Cadre n. 2006/960/JAI, du Conseil, du 18 Décembre 2006 ;
- Résolution de l'Assemblée de la République n. 71/2009 – Projet de Décision-Cadre COM (2007) 654 final SEC (2007) 1422 et 1453, relative à l'utilisation des données de registre d'identification de passagers (passenger name record – PNR) à des effets d'application de la loi pour des fins de combat du terrorisme et de la criminalité organisée ;
- Loi 81/2009 du 21 août – Crée un système de surveillance dans le cadre de la santé publique qui identifie les situations de risque, recueille, actualise, analyse et divulgue les données relatives à des maladies transmissibles et autres risques en santé publique, et prépare des plans de contingence pour faire face à des situations d'urgence ou aussi graves que celles de calamité publique;
- Décret-loi 262/2009 du 28 septembre – institue le régime juridique applicable à la base de données désignée de Registre National de Conducteurs avec la finalité d'organiser et maintenir actualisée l'information nécessaire à l'exercice des compétences spécifiques de l'Institut de la Mobilité et des Transports Terrestres, E.P., en matière de conducteurs.

SLOVAKIA

A. Legislative Developments

Within the 2009 the Office for Personal Data Protection of the Slovak Republic (hereafter referred as to „the Office“) formulated new wording of some legal provisions of the Data protection Act currently in force. The prepared draft law will amend the Data Protection Act taking into consideration recommendations resulting from the structured dialog with European Commission representatives, incentives from the application of the Data Protection Act in practice as well as the latest developments following the adoption of the Framework Decision on personal data protection processed in the framework of the police and judicial cooperation in criminal matters. The draft amendment will be submitted to Slovak government in October 2010.

B. Major Case Law

In 2009, the Office has been involved in several law suits. In two cases the Office was subject to judicial review of his decision to issue an order for remedy imposed on a controller of information system - credit provider and his processor. An order for remedy was imposed on the controller in order to stop the unlawful disclosure of the payment demand disclosed in an open delivery letter. By these proceedings, the controller made available the data revealing economic identity without legal ground. The controller has filed an action with the court with this matter upon which during 2009 the ruling has not yet been finally given. In a related case, the court is involved in handling a petition of the processor of the former controller who claims that the respective Office's decision – an order to undertake an action for remedy which in this case means to proceed in accordance with the scope and condition of the personal data processing set up by the controller in a written contract – has not been lawful. This case has also not yet been resolved by the court's final judgment.

In the third case, the Office was subject to judicial review of its decision upon the imposing of a fine on the controller. Notably, this particular controller did not manage to adopt appropriate security measures. At the first instance, the county court was addressed which decided that the imposing of a sanction was in line with the Data Protection Act. The controller referred to higher instance by appealing to the Supreme Court. This cause is still subject to the Supreme Court's decision-making.

C. Major Specific Issues

Inspection Activity and Issue of Notifications

Supervision of personal data protection in numbers

In 2009 data subjects and other natural persons who claimed a breach of the protection of their personal data filed 108 notifications with the Office. A further 36 notifications were filed by other subjects who alleged the suspicion of violation of the Data Protection Act. The Chief Inspector of the Office ordered 128 proceedings against the controllers of filing systems to be conducted ex officio. In 2009 initiated the Department of Inspection 272 proceedings. Another 39

notifications were pending from the year 2008. Overall, the Department of Inspection in 2009 dealt with 311 notifications.
In this regard the Department of Inspection in coordination with the sub-department of investigation of complaints conducted by the controllers and processors of filing systems 107 inspections and 72 'submissions to explanations'. Altogether 161 'orders' were issued for removal of deficiencies determined by the inspection. This means an increase by 120% compared to 2008. The right to file an objection against the issued order had been used only by 4 controllers which amounts only 2,5 % of the overall number of the controllers targeted by the Office's orders.
In 2009, the Office imposed 19 fines for a total amount of 27 446, 19 EUR**.**

Nationwide Inspection Activities of the Office

Inspections of the personal data processing performed by the manpower agencies (head-hunters)

During 2009, the Office effectuated several nation-wide inspection operations. One of them was the operation targeting personal data processing by the headhunting (manpower) agencies.

Headhunting agencies process not only data subjects' identification data but also the data revealing their professional as well as personality skills and characteristics. These data are acquired mainly through the internet interface or by regular post. By the inspections mainly the following facts have been examined:

- Legal base for obtaining of personal data,
- Compliance with the defined scope and purpose of the data processing,
- Information notice about the particularities of the data processing,
- Accuracy, integrity and updating of processed personal data,
- Duty to destroy personal data as soon as the original purpose of their processing has been terminated,
- Adoption of the technical, organizational and personal measures for ensuring of personal data protection, inclusive the measures preventing risks of human failures by rendering advice to the 'entitled persons' authorized to access and process of personal data.

By inspections it has been established that the data subjects by giving off of their personal data have not been duly informed by the controllers on their rights guaranteed by the Data Protection Act. The office issued an order whereby instruction to all inspected controllers to remove the shortcomings in determined time period was imposed. In two cases the Office lodged the proposal for imposing of financial sanction in the administrative procedures.

Inspections aimed at the processing of personal data by travel agencies

According to the 2009 Inspection Plan, travel agencies were also inspected. Department of Inspection examined in travel agencies analogical range of questions as in the manpower agencies and also checked whether the content of the contracts with processors was in compliance with the Data Protection Act.
Inspections proved that reviewed travel agencies processed adequate personal data for the given purpose, destroyed them in the prescribed manner and for the protection of personal data have taken appropriate technical, organizational and personal measures, except for one case. In this

case it was showed that controllers by obtaining the personal data did not sufficiently inform data subjects about their rights guaranteed by Data Protection Act.

All controllers gathered personal data of the data subjects also through processors. In two cases it was found out that contracts were not consistent with the provisions of the Data Protection Act because towards the processors they did not defined a list /scope of processed personal data and the conditions for their processing. The orders were issued by the Office in order to eliminate founded shortcomings. These orders were all met.

Special inspection activities

In relation to the accession of the Slovak Republic to the Schengen area, the Department of Inspection pursued in 2009 further inspections in the selected embassies of the Slovak Republic abroad and in the relevant offices in the Slovak Republic. The aim of the inspections was to examine compliance of the controllers of filing systems with the Data Protection Act, procedures applied while issuing Schengen visas and meeting of requirements stated in the Schengen Catalogue (recommendations and best practices) related to visa issuance.

Inspections at the consulate departments of the Slovak Republic embassies in London and Dublin were carried out in May 2009.

In the third quarter of 2009 inspections were carried out at the following departments of Border and Aliens Police Bureau (BAPB) of the Ministry of Interior of the Slovak Republic: Border Control Unit Bratislava Ružinov - Airport, Unit for Coordination of Information Systems Operation of BAPB, Border Control Unit Vyšné Nemecké, Border Control Unit Košice - Airport, Border Control Unit Poprad - Airport and Border Police Directorate Sobrance. In November 2009 inspection at the Migration Office of the Ministry of Interior of the Slovak Republic and at the Accommodation Centre Rohovce was executed which was focused on processing of personal data of asylum applicants.

Cross-border Personal Data Flow

In 2009 the Office issued eight approvals of the cross-border flows of personal data to countries which do not provide an adequate level of data protection. In case of one multinational company approvals of transfers of personal data were issued pursuant to fulfilment of requirement on accession of the data importers to the Safe Harbour principles and in remaining cases by applying the standard contractual clauses for processors in third countries in the respective contracts on transfer of personal data. There have been also cases whereby the controller – multinational company applied in particular case both Safe Harbour scheme and the standard clauses designed for processors in third countries not ensuring adequate level of data protection. The subject of cross-border data flows were mainly personal data about employees and clients of international corporations.

During 2009 the Department of Foreign Relations issued 48 written opinions to questions submitted by the controllers of filing information systems, or by the law firms representing the controllers of filing information systems. Questions were mostly related to the transfer of employment personal data, human resources management, whistle-blowing and processing of personal data of controllers' clients.

Questions were aiming to clarify the cross-border personal data flow conditions between:

- Controllers and processors based in the EU countries,
- Controllers and processors based in India and the Republic of Korea,
- Controllers and processors based in the EU countries and on the onward transfer to a third country which does not provide an adequate level of data protection,
- Cross-border data flow for the purpose of whistle-blowing.

International Cooperation

Tasks at the international level resulted mainly from the Slovak Republic's membership in the European Union and in working groups established under its auspice and from legal acts of the European Communities. Particular obligations arose from the membership of the Slovak Republic in Europol, Schengen Information System, Customs Information System, Working Group on Police and Judicial Cooperation, Coordination Working Group for Eurodac and Schengen Evaluation Working Group (SCHEVAL). In compliance with the working programme for 2009

prepared by the European Commission and the Standing Committee on the Evaluation of Schengen States, the Expert Group SCH-EVAL conducted:

- Review of enforcement of underlying principles for the processing of personal data in SIS by 'old Schengen states' (Germany, France, Belgium, the Netherlands and Luxembourg),

- Review of preparedness to implement the Schengen acquis in the field of protection of personal data in the candidate countries - Bulgaria and Romania.

The findings and recommendations formulated in evaluation reports revealed on the one hand limitations in the practical application of the SIS Convention and on the other hand responsible approach of evaluated candidate countries while attempting to meet the criteria required for entering the "Schengen area". Final evaluation reports were submitted to the Working Group for SIS/ SIRENE and the Council for its approval.

Within the framework of bilateral and regional meetings which are held to address specific issues of cooperation and for exchange of best practices the most important are as follows:

- Participation at the 11th meeting of the supervisory authorities for data protection in Central and Eastern Europe (DPA of CEE countries) in May 2009,

- Meeting with EDPS Mr. Peter Hustinx in the premises of the Office in September 2009. Mr. Hustinx was thoroughly informed about the Office's activities and with the employees of the Office discussed challenges and new priorities of the data protection in the European Union as well as the prospective possibilities of achieving the highest possible synergies of efforts of the supervisory authorities for data protection. Mr. Hustinx also visited National Council of the Slovak Republic where he met members of the Parliamentary Committee on Human Rights, Minorities and the Status of Women. On this occasion a special press conference had been organised which was devoted to his visit to Slovakia,

- Thorough exchange of best practices on the mass media policy, awareness rising and opportunities for cooperation with the Office of Personal Data Protection of the Czech Republic in Bratislava in October 2009.

SLOVENIA

NATIONAL REPORT OF THE INFORMATION COMMISSIONER OF THE REPUBLIC OF SLOVENIA Covering the year 2009

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

In Slovenia the modern legal and institutional framework for data protection (and access to public information) has been established and for years already coherent with the *acquis communautaire*.

Authorized by the special provision of the Article 48 of the Personal Data Protection Act[4] (PDPA) the Information Commissioner issued several preliminary opinions on legislation in preparation regarding the compliance from the aspect of personal data protection. One of the important achievements of the Information Commissioner are the amendments and supplements of the Electronic Communications Act[5] (ECA) passed at the end of 2009. The amendments include the provision on anonymisation of telephone numbers included in the itemised bill received by subscribers as provided by the e-Privacy Directive (2002/58/ES). The recommendations of WP29 (WP 113) regarding the provisions of Data Retention Directive (2006/24/ES) were also taken into account. The data retention period is now shortened to 8 months and must not exceed 14 months. The amended ECA also limits the retention period for the supplied retained data and the registration of supplied retained data from the previously indefinite period to the limited period of 10 years. One of the most important changes of the ECA are the provisions on supply of traffic and location data to the police in the events of life and limb protection and on the Information Commissioner's competence to oversee the provisions on lawful interception of communications.

The other major pieces of legislation considered by the Information Commissioner in 2009 were the laws concerning general administrative procedure, criminal procedure, aliens, passport, state border, banking, foreign affairs, health, police, Red Cross, family code, money laundering and terrorist financing prevention, archives, etc.

B. Major case law

Similar to previous years in 2009 the Information Commissioner dealt with several cases widely publicized by the national media.

Political parties

The Information Commissioner initiated an inspection procedure against two political parties in Slovenia because of a suspected illegal collection and detention of personal data for the purpose of the electoral campaigning. The complaint came from a number of Slovenian citizens/registered voters living abroad, who received direct marketing material from the two political parties

[1] Official Gazette of the RS, No. 94/2007
[5] Official Gazzete of the RS, No. 13/2007

without having given their consent to the parties to use their contact data for marketing purposes. In the course of the inspection procedure the political parties could not prove legal basis for the collection of the citizens' contact data. As a consequence of the established violation the Information Commissioner fined the two parties with a 4.170 € fine each. The liable persons in the parties were also fined, 830 € each.

President of the District Court

President of the District Court was found liable to pay a fine of 1660 € because of two offences of unlawful processing of personal data. It has been established in the offence procedure that the liable person has been collecting and further processing data on calls made from work telephones (traffic data) of two employees. The purpose of processing these traffic data was not defined or lawful, and further processing was not consistent with the law. The Information Commissioner's decision is not final yet. Pursuant to the provisions of the Courts Act the Higher Court also conducted a supervision of the work of the court management at the mentioned District Court.

Since this case has merely reflected widespread problems in the field of privacy at workplace the Information Commissioner once again expressed it's view that this field requires better legal framework as practically one third of all cases in the Information Commissioner's competence touches upon workplace privacy.

Unlawful supply of personal data among two insurance companies

The Information Commissioner fined two insurance companies and the liable persons for unlawful processing of personal data. In the offence procedure the Information Commissioner established that personal data of 2382 individuals have been supplied without legal basis provided by law or personal consent of the affected individuals.

The insurance company that supplied the personal data was fined for unlawful supply of personal data and for insufficient traceability of the supplied data. The Information Commissioner found conclusive evidence that data on 26 individuals have been processed unlawfully and therefore the company was fined with 112.590 € and the liable person with 20.000 €. The company filed a request for judicial review. The other insurance company was fined for unlawful acquiring of personal data with 108.420 €, and the liable persons with 20.000 € each. This company took advantage of the option provided by law and paid half of the fines immediately.

These are the highest fines imposed by the Information Commissioner so far. The Information Commissioner emphasised that in the future such unlawful supply of personal data among the controllers that are in possession of sensitive personal data or of large data bases will be strictly sanctioned.

Data protection in banks

The Commissioner conducted a systematic supervision over security of personal data in the banking sector (6 of the biggest banks), namely the lawfulness of processing of personal data in the inter-bank transfers of clients credit rating data included in the new SISBON system and the lawfulness of access to clients' bank account data. The Information Commissioner established that in the context of inter-bank transfers of data no unlawful accesses to data have been made,

however unauthorized accesses to the data on some well known clients' (politicians) bank accounts have been made in two of the banks included in the supervision. The un-authorised employees who have accessed data on clients' bank accounts have been sanctioned pursuant to the General Offences Act.

Journalist's e-mail and questions published on the Information Commissioner's website

The Information Commissioner published on his website an e-mail received from a journalist containing journalistic questions and the journalist's work e-mail address. The journalist's e-mail was also sent to a number of subscribers on the Information Commissioner's mailing list. The journalist filed a complaint however the Information Commissioner found no breach of the Data Protection Act and did not initiate an inspection procedure. The reasoning of the Information Commissioner was that the e-mail was sent to the Information Commissioner's official work e-mail address, established to receive e-mails from natural and legal persons concerning the work area of the Information Commissioner. The name, surname and work e-mail address of the journalist in this case did not represent protected personal data, as the journalist was acting in his public journalistic role, with his name published on the official website of the media. His privacy and dignity have therefore not been prejudiced by the publication of his e-mail. The questions contained in the e-mail concerned the public nature of the Information Commissioner's work and additionally the contents of the communications were meant to be published. That's why the journalist's questions could not be regarded as protected personal communication but rather as public information.

A judicial decision published in the newspaper

A part of a judicial decision containing the plaintiff's personal data was published in one of the Slovenian dailies. The Information Commissioner found a breach of the Personal Data Protection Act and fined the newspaper company and the liable person. The case is important because the Information Commissioner has taken the position, that personal data contained in a judicial decision pertaining to a non-public figure represent protected personal data. The judicial decision may therefore only be published in anonymised form. The Information Commissioner has also taken the position that in the event of the collision of the right to freedom of expression and the related constitutional principle of publicity of trial and the right to data protection in this case the right to data protection of the non-public figure prevails. The public interest is not equal to what public is interested in and the sole curiosity of the public must not justify intrusions of the constitutional right to information privacy.

C. Major specific issues

In addition to the role of the inspection supervision body and offence body, the Commissioner has been conducting various other tasks with regard to the provisions of PDPA.

Since the performing of **biometric measures** is allowed only after the receipt of the Information Commissioner's decision the total of only 10 applications were received in 2009 (compared with 16 in 2008 and even 40 applications in 2007). Proportionally, a decrease was noted in the number of decisions issued – 6

decisions (4 granted, 2 refused) compared with 17 decisions in 2008 and 35 decisions in 2007.
An unchanged situation in 2009 compared with the previous year has been noted in granting permits for the **connecting of filing systems**: a total of 8 decisions were issued equally in 2009 and 2008 (7 in 2007) regarding the connecting of filing systems.
In 2009, 71 complaints were lodged with the Information Commissioner as a competent body for deciding on the appeal of data subject concerning the **right to information**.
By the end of 2009 the personal data filing systems of more than 11.000 controllers were registered in the **public Register** which is managed by the Information Commissioner and published on its web site. The figures show an increase of some 1000 new entries per year.
In the framework of its **inspection activities** (as of December 2009, there are nine state supervisors for data protection - inspectors employed with the Commissioner) in 2009 the Information Commissioner received 624 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act, thereof 219 (256 in 2008) in private and 405 (379 in 2008) in public sector. Compared with previous years (635 cases in 2008, 406 cases in 2007 and 231 in 2006) a dramatic increase in caseload as of 76% in 2007 and 56% in 2008 has been ceased. Similarly to previous years most complaints pertained to unlawful or excessive collection of PD, disclosure of personal data (PD) to unauthorized users, illegal video surveillance, insufficient PD protection, unlawful publication of PD etc. In 163 cases the administrative offence procedures were initiated (279 cases in 2008 and 133 cases in 2007).
In 2009 the number of requests for **written opinions** and clarifications amounted to 596 exhaustive written answers and 1471 short answers by the Information Commissioner (apart from several hundreds of oral answers by phone). Compared with 853 cases in 2008 or 1144 cases in 2007, these figures have evidently been reflecting the persistence of a high level of public awareness of the right to privacy brought to effect by a modern Personal Data Protection Act and also by the transparent work and intensive public campaigning of the Information Commissioner.
In addition to publishing non-binding opinions in the form of written explanations on his website and besides publishing a number of brochures on matters of data protection, in 2009 the Commissioner has continued publishing its **Guidelines** on specific matters of data protection. The purpose of the Information Commissioner’s guidelines is to provide common practical instructions and information for public, data subjects and controllers in a form of typical frequently asked questions and answers to comply with the statutory provisions of the Personal Data Protection Act and/or other legislation. Last year the Commissioner prepared and published on his website the guidelines regarding the code of conduct in handling personal data collection, protection of personal data in relation to the media, informing and awareness raising of the consumers, identity theft, data protection of children in school, prevention and protection from cyber bullying and social engineering.

In the context of the Third European **Data Protection Day** which in 2009 coincided with its 5th anniversary the Commissioner already traditionally organized a round table debate, this time on the topic “Privacy in the workplace”. For the third time the Commissioner awarded subjects from public and private sector for good practice in personal data protection. The awards for excellence in data protection were presented to the company Cetis d. d. and to the Ministry of Defence of the Republic of Slovenia. Additionally, for the first time, awards were presented also to companies that have proved a high level of personal data security with an ISO/IEC27001 certificate for information security.

International cooperation

Permanent cooperation in the bodies of the European Union and the Council of Europe

The Information Commissioner as the national regulatory body in the field of data protection permanently cooperates with the competent bodies of the European Union and the Council of Europe in the field of data protection. The Information Commissioner is bound to the international cooperation by the provisions of the Directive 95/46/ES.

In the 2009 the Information Commissioner has actively participated in 5 working bodies at the level of EU, concerning supervision over data protection in the EU in different areas. These encompass: the working group for the protection of personal data under Article 29 of the European Data Protection Directive, the joint supervisory bodies for Europol, the Schengen area and the customs information system, as well as the co-ordination meetings of the European Data Protection Supervisor together with national bodies for the protection of personal data and supervision over EURODAC.

The Information Commissioner has been in 2009 elected vice president of the joint supervisory body for Europol, and within the scope of police and judicial co-operation the Commissioner regularly attended meetings of the Working Party for Police and Justice.

With the entrance of Slovenia into the Schengen area the Information Commissioner became the independent body which oversees the transfer of data for the purpose of the convention and its competencies extended to oversight of the Article 128 of the Schengen Convention. In 2009 55 requests for access to personal data have been received and none of the requests were denied. The Information Commissioner has not received any complaints regarding the execution of the right of the individuals to access their data contained in SIS at the first level.

In 2009 the Information Commissioner participated in the inspection supervision group for Schengen evaluation of Bulgaria and Romania to enter the Schengen area in the framework of SCHEVAL.

In the context of the Council of Europe a representative of the Information Commissioner participated in the Council of Europe’s Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). This year the Council was mostly working on the Draft recommendation on the protection of individuals with regard to automatic processing of personal data in the framework of profiling.

The Information Commissioner also actively participated in the Internet and Information Technology Sub-Group under the auspices of the European Data Directive Working Group. The working group adopted two important documents in the 2009, namely the Recommendation on Data Protection and E-Waste and Report and Guidance on Road Pricing – “Sofia Memorandum”. The Sofia memorandum was initiated with the recommendation of the Slovenian Information Commissioner. The international working group IWGDPT continues the work in the fields such as Deep Packet Inspection, geolocation data, social networking sites and others.

Other international cooperation

The Information Commissioner's representatives have also participated in the following important **international events**:

Barcelona conference "High level meeting for joint proposal for the drawing-up the international standards for privacy and data protection"
Spring Conference on personal data protection, Edinburgh
2nd European Privacy Open Space and "re:publica", Berlin
Data Protection Conference 2009, Brussels
11th Meeting of the Centraland Eastern European Data Protection Commissioners, Romania
Open Society Institute Meeting on Freedom of Information, Budapest
Strengthening Data Protection in Israel, Tel Aviv (twinning project)
International Conference of Information Commissioners, Oslo
XXth Case Handling Workshop, Limassol
Third Privacy Open Space Conference, Vienna
31st International Conference of Data Protection and Privacy, Madrid.

The Commissioner built on **bilateral cooperation** mainly with Hungary, Serbia and Monte Negro.

All these efforts and achievements have also been resulting in a high rating the Commissioner permanently enjoys in terms of its reputation, public trust and public awareness of its activities which is also reflected in the findings of public opinion polls. According to the latest results (January 2010) of the survey on public trust carried out by the Slovenian Public Opinion Research Center the trust in Information Commissioner is even evidently growing. Among other measured institutions, the only institution that is more trustworthy than Information Commissioner is the official currency – Euro. With a high degree of public trust (53.1 %), the Commissioner left behind all other institutions, such as Military, the President of the Republic, the Ombudsman, Schools, Police etc. It is also worth mentioning that Information Commissioner enjoys the lowest rate of public distrust among all the institutions included in the survey.

In May 2009, the National Assembly of the Republic of Slovenia has, upon the proposal of the President of the Republic elected Mrs. Nataša Pirc Musar for another 5 year term as the Information Commissioner with great majority of votes.

SPAIN

Current situation and future perspectives

1. A MORE INFORMED SOCIETY MORE CONSCIOUS OF ITS RIGHTS

A) Greater social awareness regarding the risks of Internet.

In order for citizens to benefit from effective protection in the use of their personal data not only must they know the rights which the regulations recognise for them and the manner in which these may be exercised but they must also keep their degree of awareness "updated" in the light of the new risks that affect their privacy, foremost among which are those generated by technological development and the new Internet services.

The data of the Sociological Research Centre (CIS) barometer for September 2009 on trust in the Internet reveal that 56% of citizens think that security and privacy in the Web is low or very low, confirming that citizen concern regarding the risks of the Internet is a confirmed reality.

The Spanish Data Protection Agency (AEPD), for its part, has redoubled its efforts to improve the knowledge of citizens on this subject and to make measures available to avoid the risks. In this respect, it has carried out a joint study with the National Institute of Information Technologies (INTECO) on the privacy of personal data and security in online social networks and has updated a guide with recommendations to Internet users which analyses the main risks that are currently present in the Web.

But there is no doubt that mass media have played a decisive role in raising citizen awareness, focusing on the impact of new technologies on the privacy of individuals and, specifically, on the risks associated with services such as social networks. The AEPD has recognised this work of dissemination by granting its 2009 communication and dissemination awards to programmes such as "12 months 12 causes" by the television channel Telecinco, the weekly section on data protection on "Radio 5 Todo Noticias" and a documentary project to inform minors with regard to new technologies.

B) Citizens, more aware of their rights.

The CIS barometer indicates that citizens have more and more knowledge of their rights. Thus, the concern for data protection and the use of personal information has grown, reaching 74.1% of those surveyed. The percentage of citizens who know of the existence of the Spanish Data Protection Act (LOPD) is around 50%, and the same occurs with the AEPD as the organisation that guarantees their rights, which for the first time exceeds the 50% barrier.

The greater awareness by citizens is resulting in a growing demand for the guarantee of their rights. A significant example is the growth of almost 34% in the number of consultations placed with the Citizen Attention Service, by telephone, in person or in writing, approaching in 2009 the figure of 100,000. Likewise, visits to the web page of the AEPD increased by 700,000 compared to 2008, reaching 3,000,000, which means a daily average of 8,214 visits. The number of

consultations of the General Data Protection Register has also experienced considerable growth in the last 12 months, the total figure being around 2.5 million.
The analysis of the consultations placed indicates that video-surveillance has become one of the outstanding concerns of citizens, combined with advertising and credit reporting, or information regarding access to medical records. But other doubts are beginning to gain relevance, regarding what to do so that personal data disappear from a web page, whether it is obligatory to register the geolocation files of employees, or whether Bluetooth scanning which reports information on mobile telephones is included in the LOPD.
A survey by the AEPD reveals that almost 90% of citizens declared that they felt satisfied or very satisfied with regard to the waiting time in order to be assisted and regarding the attention received. The satisfaction index regarding the information received, the knowledge and manner of the helpline operator of the AEPD varies between 99.88% and 100%.

C) New concerns: How do I disappear from a web page? Must I resign myself to being visible in the Internet? How do I exercise my right to oblivion?

The AEPD observes that the greater knowledge of data protection regulations corresponds with more active behaviour by citizens in the exercise of their rights before those who process their personal information. In this respect, an increase of almost 14% can be appreciated in requests for the safeguard of rights, in the region of 2,000. Requests for erasure of data or object to their processing by Internet browsers, still not very numerous, have increased by 200%.
In the light of the question, Must I bear being visible in the Internet? the reply is no. The decisions pronounced by the AEPD take the line of requiring that the necessary measures be adopted to avoid the indexing of personal data, likewise taking into account the possible actions that webmasters may adopt to make effective the right requested by the individual.
But, aside from these matters, the main questions that citizens continue to ask are: Who has my data? How can I erase them? This is shown by the considerable increase in the decisions relating to the safeguard of the rights of access (59%) and erasure (40,8%), these latter adding up to a total of 1,366 decisions. Another new development is the sharp increase in decisions regarding the right to object (470%).

2. GUARANTEE EFFECTIVE AND EFFICIENT COMPLIANCE WITH THE LOPD

A) Facilitate compliance with the law: a guarantee for citizens.

Informative policy has been intensified in the conviction that facilitating compliance with the law results in an increase in the guarantees to citizens. Thus, in January 2009 the 2nd Annual Open Session was held, which was attended by around 700 participants and the catalogue of practical guides has been expanded, publishing new editions with recommendations to Internet users,

video-surveillance and data protection in the workplace and, in English, the guides on video-surveillance and the rights of boys and girls and the duties of fathers and mothers.
The Helpline continues to be a very useful channel in the informative policy of the Agency, as is shown year after year by the increase in consultations. The Legal Department, for its part, attended to a total of 679 consultations, of which 359 (54%) were placed by the Public Administrations and 313 (the remaining 46%) by the private sector.
These policies continue to give results. In 2009, almost 400,000 files were registered in the General Data Protection Register (RGPD), which implies an increase of over 50% compared to 2008, reaching a total figure of 1,647,756. One contribution to this increase has been the simplified file notification system NOTA, which facilitates notification via the Internet, something which is used in almost 90% of manual notifications. Furthermore, the use of digital certificates is gaining ground, to the point that this format is used in one in five notifications.
The increase in registrations is strongest in the private sphere, which has grown by 63%, whilst in the public sector an increase of almost 50% can be highlighted in Local Administration files, owing to which the files of municipalities in the RGPD represent almost 96% of the Spanish population.
The offer of new channels to facilitate compliance with the law has given a qualitative leap in the EVALÚA program, an online self-test for self-assessment of compliance with the LOPD for companies and local authorities, which offers free of charge answers to the doubts which habitually confront those who process personal data.

B) A permanent zeal for legal certainty:

The AEPD has continued working to achieve greater legal certainty via its mandatory opinions on provisions of general application. 100 provisions have been reported on, such as the draft bills on money laundering and the financing of terrorism, or that of simplification of information and intelligence between the security services of the Member States of the EU. Opinions have also been prepared on the agreements of the EU with Australia and the USA regarding the processing and transfer of EU sourced Passenger Names Records (PNR).
Moreover, the analysis of the degree of legal certainty in the application of the LOPD obliges contemplation of the extent to which the decisions of the AEPD are ratified or revoked by the Courts. In relationship with the appeals regarding the erasure of data in the Baptism Records of the Catholic Church, during 2009 99 rulings have been issued in the first instance by the Spanish National Court (29% of the total) and the Supreme Court has judged 163 appeals (more than 90% of the total) in the sense upheld in its ruling of 19 September 2008.
Not including the rulings mentioned, in 2009 the contentious-administrative chamber of the Spanish National Court and the Supreme Court have issued 240 and 19 rulings, respectively. Regarding the rulings of the National Court:

- 162 dismissed the appeals brought against decisions of the Agency (which were fully confirmed) (68%)
- 17 partially upheld the appeals (7%)
- 61 wholly upheld the claims to set aside the decisions of the Agency (25%)

For its part, and also without referring to the rulings on the Baptism Records of the Catholic Church, the Supreme Court ratified the criteria of the Agency on 16 of the 19 occasions on which the matter was subjected to its judgment.

C) A growing demand for guarantees: an active response by the Agency.

The number of claims brought before the AEPD in 2009 has caused an increase of 75% in the actions brought, exceeding 4,100 (where telecommunications, financial institutions and video-surveillance have been the main sectors investigated).
However, in decisions on sanction procedures against private organisations, telecommunications and financial institutions, despite occupying the first and third place based on the number of proceedings, have decreased by 10.34% and 21.26% respectively. On the other hand, private video-surveillance for security reasons rises to second place, with a 229.55% growth on the previous year. The decisions which declare a breach of the LOPD by the Public Administrations have increased by around 12.5%.
The amount of the sanctions imposed amounted to 24,872,979.72 euros. Although this figure represents an increase of 12.99% compared with the previous year, it is close to the volume of sanctions declared in the year 2006, with the relevant difference that the number of sanction procedures resolved in 2009 is higher than that of 2006 by 235%. It is precisely the considerable increase in sanction procedures and not the sum of the sanctions declared that explains the figure of the sanctions imposed. Minor sanctions are those which present the greatest increase (44.76%), whilst serious ones remain stable and very serious sanctions decrease by almost 6%. Regarding the total of the sanctioning decisions, a qualified reduction of the liability of the offenders can be seen in 40.72% of the cases.
Analysing the data that have been presented it is appropriate to conclude that the quantitative increase in the sanctions, a consequence of the previous increase in complaints, does not hinder appreciation of the improvement in compliance with the LOPD, with the growth in breaches for reasons of form, the reduction of very serious breaches and the reduction of liability when a breach is committed.
The 2008 Annual Report included citizen concern regarding the receipt of advertising by telephone. To give an efficient response to this question, the AEPD has promoted, together with the Spanish Federation of Electronic Commerce and Direct Marketing (FECEMD), a new opt-out file so that those who do not wish to receive advertising may express this and choose the channels via which they wish to receive advertising, whether by post, e-mail, SMS, MMS or telephone. From the information requested from FECEMD the number of persons

registered in the Robinson List service amounted to more than 110,000 at 31 December 2009. The implementation of the service is a palpable demonstration of the efficiency of the preventive policies and collaboration with those obliged by the LOPD to increase the guarantees to citizens.
Furthermore, in an environment of economic crisis such as that which developed during 2009, an exponential increase has taken place in actions deriving from or related to claims for default.
Mention must also be given to the very considerable increase in the invoking by citizens of the defence mechanisms granted by the LOPD in the light of undue processing of their personal data in the sphere of creditworthiness. The number of procedures for the protection of data subjects' rights brought on this matter increased by 570% and that of preliminary actions prior to possible sanction proceedings by 225%. In the sphere of the assignment of receivables between companies, also known as sale of debt, various sanction procedures have been resolved which have derived in the imposition of sanctions that have reached up to 420,000 Euros. Likewise, it is appropriate to highlight the existence of various complaints against possible practices which violate the duty of secrecy in actions of recovery, via the disclosure of the debt to family members or relatives to force the collection of an allegedly owed sum.

3. PRIVACY AT RISK: THE BIG QUESTION-MARKS

A) Internet. New services, new challenges.

The consideration for the free use that users make of Internet services is the unilateral establishment of terms and conditions by the service provider. Therefore, priority should be given to those active policies aimed to establish relations with the providers of these services. In this respect, the AEPD has communicated to Facebook and Tuenti the recommendations of the study prepared with INTECO, insisting on the improvement of privacy policies so that they offer clear and understandable information, and on the need to set up privacy policies by default and erase all the contents of the profile as soon as un-registration is requested.
In 2009 156 proceedings were brought regarding preliminary proceedings specifically related to services provided via Internet. A new aspect is the fact that 18 of these proceedings were instituted as a consequence of 31 complaints related with users of the social networks *Facebook* and *Tuenti*, the majority referring to the dissemination of photographs of third parties without their consent.
The majority of the rest of the actions are also related with the unauthorised dissemination of personal data via Internet: 37 of them refer to forums or blogs, 13 to video hosting services, fundamentally *YouTube*, and 38 to other types of website such as corporate sites, collections of law reports or personal sites. Another 28 claims are related to advertisement websites, online dating services or electronic mail services. In the majority of cases they are related with the unauthorised dissemination of data.

Likewise, 10 of the actions deal with incidents of various types related with online shopping or with electronic commerce operations. Finally, it is appropriate to mention 5 preliminary proceedings brought in relation to web search engine services and the location of personal information in directories or in people search engines.

B) Minors. A necessary protection in the light of their growing presence in the Web:

The use of social networks has become a habitual activity for the social development of minors, to whom they offer access to a new means for contacting each other. The risk for them is that, to a great extent, they start out with a basic educational deficit regarding the lack of knowledge of how to exercise real control over their information.
Data protection regulations do not allow minors under the age of fourteen to register as users of a social network without the consent of their parents. The Agency has assumed compliance with this obligation as a priority. In fact, in the meetings held with those responsible for Tuenti and Facebook, the control of access by minors has been a permanent demand.
In reply to the demands of the AEPD, Tuenti presented an age verification system that analyses the profiles of suspect users, erasing those who do not prove that they are 14 years old. Likewise, it has undertaken to strengthen the purging processes of existing profiles and to develop systems for the verification of new suspect profiles. Furthermore, it has issued information regarding the modification of the privacy policy, establishing by default the maximum level of privacy for users under the age of 18. Likewise, the Agency requested those responsible for Facebook to increase the age limit to 14 years for users in Spain.
However, it is necessary to incorporate in syllabi adequate training on data protection and privacy, as well as for Public Administrations and schools to make technologies available to pupils that limit access to Web services by the under-14s. In this context, the electronic Identity Document is proving to be one of the most efficient instruments for accrediting age in the Internet. This Agency considers it to be extremely important that the adequate initiatives be implemented in order for over-14s to have the digital means available to allow them to prove that they have the required age to give their consent to the processing of their data.

C) Video-surveillance: living with guarantees.
Video-surveillance for security reasons has become an omnipresent reality. Each year significant growth takes place of video-surveillance files, as in 2009, when the files registered in the General Data Protection Register which declare this purpose increased by around 240% in the private sphere exceeding the figure of 37,000. In the public sphere the increase was 60% with a total of 578 files.
The 2009 survey of the CIS reflects that 68.7% of citizens are in favour of their installation, whilst 10% are against. However, more and more people lodge complaints of breaches of the LOPD in relationship with video-surveillance, where the sanction procedures resolved have increased by 230%.

Furthermore, the recent enactment of the Act 25/2009, of 27 December, for the modification of various laws for their adaptation to the Act on free access to service activities, has extended the legitimisation for the installation and use of video-surveillance devices. This will presumably give rise to a reduction of the sanctioning decisions of the AEPD, the said fault of legitimisation being one of the most frequent breaches.
Regarding cameras that allow images to be transmitted via the Internet, the AEPD carried out a sectoral inspection, noting that the majority allow identification of the persons filmed. The main deficiency detected is that, habitually, the control mechanisms for access to the images are disabled by the manufacturer or are activated with a default username and password. The lack of diligence in access control causes a vulnerability that allows access by third parties by leaving the camera in an “open door” situation. A catalogue of recommendations is offered, among them the need to activate the control of access to the images with username and password. The inspection has led to the bringing and resolution of 7 sanction procedures.

D) Employment context: balance between rights and obligations.
The variety of processing of personal data carried out in the employment sphere has led the AEPD to prepare a guide on data protection in companies, to provide an answer to practical aspects which companies must habitually confront, suggesting criteria that allow compliance with personal data protection regulations. The guide includes specific recommendations on the processing of specially protected data, in particular, those on health and trade union membership, as well as the guarantees that should be observed in occupational risk-prevention.
Although not necessarily dealing with personal data, it also incorporates recommendations so that the implementation of internal whistleblowing schemes in the company is carried out while guaranteeing the protection of the employees. The chapter dedicated to employer controls indicates the rules applicable to biometric controls, video-surveillance in the workplace or on the use of technological tools provided by the employer and, also, those related to the control of occupational absenteeism.

E) International data flows. Flexibility and globalisation.

International data transfers from Spain have globalised and reach all the geographical areas of the world. The number of authorisations increased by 25%, the USA being the first destination country, despite the reduction in the number of transfers. Strong growth can be seen of over 100% to Latin-American countries (132 authorisations), whilst Asia maintains a constant volume of authorisations (115). In the African continent international transfers focus on Morocco (19) and the Republic of South Africa (3) and Australia appears as an emerging destination
The search for more flexible procedures for the authorisation of international transfers has advanced in 2009. The AEPD authorised the first transfer based on binding corporate rules (BCR) and has participated via a coordinated procedure

in ten requests with this type of guarantee presented before other Authorities of the European Union.
To conclude, it can be affirmed that we are witnessing a constant increase in international data flows with a great weight of the delocalisation of services and with more flexible authorisation procedures. From this we can deduce the urgent need to achieve binding standards to guarantee the protection of privacy in a globalised world.

4. 2009: MADRID, WORLD PRIVACY CAPITAL. THE MADRID RESOLUTION: A MEETING POINT FOR A GLOBAL REGULATION.

In 2009 the AEPD organised the 31st International Conference of Data Protection and Privacy Authorities – the largest forum dedicated to privacy at world level and a meeting point between data protection authorities and guarantors of privacy from the whole planet, as well as representatives of public and private bodies and civil society – converting Madrid into the world privacy centre between 2 and 6 November. It was attended by more than 1,000 people from 83 countries
This Conference, inaugurated by their Highnesses the Prince and Princess of Asturias, took place in the Congress Palace of Madrid, under the slogan “Privacy: today is tomorrow”. The nearly one hundred speakers, divided into twenty sessions, included the Spanish Interior Minister, Alfredo Pérez Rubalcaba and the Secretary of Homeland Security of the United States, Janet Napolitano, Martin Cooper (inventor of the mobile telephone), Vinton Cerf (co-inventor of the TCP/IP family of Internet protocols) as well as the Minister of Industry, Commerce and New Technologies of Morocco, Ahmed Reda Chami. However, the greatest achievement of this edition has been to manage to advance towards a universal and binding legal instrument on the subject of privacy, that contributes to a greater protection of individual rights and freedoms in a globalised world and which benefits from the widest institutional and social consensus.
Via the adoption of the designated “Resolution of Madrid”, a large step was taken along this line: the “Joint proposal for a Draft of International Standards for the Protection of Privacy with regard to the Processing of Personal Data”. This proposal aims, on the one hand, to promote the right to data protection and privacy internationally, offering a model of regulation that guarantees a high level of protection and which, at the same time, may be assumed in any country; on the other hand, it seeks to facilitate the flow of personal data at international level, trying to mitigate the existing obstacles.
Despite not being an international agreement or a legally binding regulation, its value as a reference text is justified not only by the ample participation of the international data protection and privacy community in its preparation, but also because it includes elements that are present in all the valid data protection systems currently in force, as well as by the fact that it has been backed by all the Authorities that attended the International Conference. Therefore, the promotion and dissemination of this text among private bodies, experts and

national and international public organisations will be one of the priorities of the AEPD during the year 2010.