



Strasbourg 18 December 2009

T-PD (2009) RAP 25 prov

**CONSULTATIVE COMMITTEE OF THE CONVENTION  
FOR THE PROTECTION OF INDIVIDUALS WITH REGARD  
TO AUTOMATIC PROCESSING OF PERSONAL DATA [CETS 108]**

**(T-PD)**

25<sup>th</sup> meeting  
Strasbourg 2-4 September 2009

**DRAFT MEETING REPORT**

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

## TABLE OF CONTENTS

I.	OPENING OF THE MEETING .....	3
II.	ADOPTION OF THE AGENDA .....	3
III.	STATEMENT BY THE SECRETARIAT .....	3
IV.	ELECTIONS OF THREE MEMBERS OF THE BUREAU .....	4
V.	PROFILING.....	4
VI.	DISCUSSION AND APPROVAL OF FUTURE T-PD ACTIVITIES.....	5
VII.	PRESENTATIONS.....	6
VIII.	DISCUSSION AND ADOPTION OF THE DECLARATION ON THE JOINT PROPOSAL FOR DRAFT INTERNATIONAL STANDARDS ON PROTECTION OF PRIVACY WITH REGARD TO PROCESSING OF PERSONAL DATA .....	6
IX.	DATA PROTECTION DAY .....	7
X.	INFORMATION ON 2009 DATA PROTECTION DAY AND MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD SINCE THE 24 <sup>th</sup> T-PD MEETING (13 and 14 March 2008).....	7
XI.	DATA OF THE NEXT PLENARY SESSION.....	7
-----		
	APPENDIX I - AGENDA.....	8
	APPENDIX II – LIST OF PARTICIPANTS.....	11
	APPENDIX III – WORK PROGRAMME FOR THE T-PD FOR 2009 AND BEYOND .....	16
	APPENDIX IV - STATEMENT ON THE JOINT PROPOSAL FOR A DRAFT OF INTERNATIONAL STANDARDS ON THE PROTECTION OF PRIVACY WITH REGARD TO THE PROCESSING OF PERSONAL DATA .....	20
	APPENDIX V - EUROPEAN PRIVACY ASSOCIATION PRESENTATION .....	22
	APPENDIX VI - CETS No.: 108 – State of signatories and ratifications.....	26
	APPENDIX VII - CETS No.: 181 – State of signatories and ratifications.....	28
	APPENDIX VIII - INFORMATION ON RECENT DEVELOPMENTS AT NATIONAL LEVEL IN THE DATA PROTECTION FIELD .....	30
	APPENDIX IX – INFORMATION ON THE 2009 DATA PROTECTION DAY .....	65

## **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 (CETS 108), held its 25<sup>th</sup> meeting at the Council of Europe in Strasbourg from 2 to 4 September 2009 with Ms Eva Souhrada-Kirchmayer (Austria) in the chair.
2. The list of participations is reproduced in Appendix I to this report.

## **II. ADOPTION OF THE AGENDA**

3. 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**

The T-PD:

4. took note of the information provided by the Secretariat on new developments since its previous meeting (13 and 14 March 2008) in the Organisation in general and in the data protection field in particular;
5. noted that at the date of the meeting, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (hereafter Convention 108) had been ratified by 41 States and the additional protocol by 25 member states of the Council of Europe;
6. noted that new contracting parties had been admitted since the ratification of Convention 108, namely the Andorran and Moldovan delegations, as well as new observers, ie the Ibero-American Data Protection Network and the International Conference of Data Protection and Privacy Commissioners;
7. took note of the decision taken by the Committee of Ministers on 2 July 2008 encouraging States with the appropriate level of data protection legislation to accede to Convention 108;
8. took note of the decision taken by the Committee of Ministers on 11 March 2008 instructing the European Committee on Legal Co-operation (CDCJ) to prepare a draft recommendation on profiling in close co-operation with the T-PD. The proposed co-operation would help place all standard-setting activities in the data protection field under the same umbrella (that of the T-PD) and at the same time enable the competent steering committee to verify the overall coherency of the draft legal instruments by ensuring that the views of all member states were taken into account;

9. took note of the proposals put forward by Mr Karel Neuwirt, the Council of Europe's Data Protection Commissioner, during his visit on 15 July 2009 in connection with the review of the Commissioner's status within the Council, and decided to consider his proposed amendments to the Secretary General's regulation of 17 April 1989. It was decided that the T-PD should conduct a preliminary examination of the amendments;

10. noted that the first seminar of the second series of seminars on data protection in the context of criminal proceedings, organised by the Council of Europe and the University Castilla – La Mancha, would be held in Strasbourg from 7 to 9 October 2009;

11. took note of the wish expressed by the Luxembourg, Liechtenstein and Swiss delegations to ensure T-PD representation in the work of revising the Council of Europe Convention on Mutual Administrative Assistance in Tax Matters (CETS 127).

#### **IV. ELECTIONS OF THREE MEMBERS OF THE BUREAU**

12. Following the resignation of three members of the Bureau elected in 2008 (Ms Pascale COMPAGNIE (France), Ms Eva SILBERMANN (Germany) and Ms Stefania CONGIA (Italy), fresh elections were held in accordance with Article 10 bis § 2 of the T-PD Rules of Procedure.

13. Following a call for candidatures from the Secretariat prior to the meeting, five applications had been received from Ms Kinga SZURDAY (Hungary), Ms Nevena RUZIC (Serbia), Mr Kevin FRASER (United Kingdom), Ms Alessandra PIERUCCI (Italy) and Mr Georges GRIGORE (Romania). Of these five candidates, and in accordance with Rule 10 bis 2 of its Rules of Procedure, the T-PD elected Mr Kevin Fraser (United Kingdom), Ms Alessandra Pierucci (Italy) and Mr Georges Grigore (Romania) as Bureau members for a term of office extending until 2010.

#### **V. PROFILING**

14. The T-PD considered the comments submitted by the contracting parties and observers on the 3<sup>rd</sup> draft recommendation on the protection of individuals with regard to automatic processing of personal data in the framework of profiling (hereafter "the recommendation").

15. After discussion, the T-PD decided to restrict the scope of the recommendation to the collection and processing of personal data relating to profiling in the private sector. A provision was included encouraging member states to extend its scope to personal data collection and processing in the public sector.

16. The T-PD approved the text of the draft recommendation as established on the basis of the discussions at the 25<sup>th</sup> plenary meeting, and decided to call for comments. These comments would be discussed at the next two Bureau meetings. The draft recommendation emerging from these meetings would be transmitted for vote at the next plenary session in 2010.

17. The draft explanatory memorandum to the recommendation would be sent to representatives and observers for comments. The comments would be discussed at the next plenary meeting in 2010.

## **VI. DISCUSSION AND APPROVAL OF FUTURE T-PD ACTIVITIES**

18. The Secretariat had prepared and distributed a draft programme of future T-PD work before the meeting.

19. The discussion on the document had been preceded by statements by the representatives of the Secretariat of the Steering Committee on the Media and New Information Services (CDMC), who had come in order to present the work of this Committee. They had stressed the importance of being able to combine the possible use of new technology with the right to respect for private life, and to regulate the on-line social network sector. This highly useful work might be based on close co-operation not only with the member states but also with private sector representatives. The representative of the International Chamber of Commerce had appealed to the T-PD to engage in close co-operation with the private sector.

20. The dates of EuroDIG and the Forum on Internet Governance were communicated.

21. The European Commission representative had provided an overview of the documentation on regulating the functioning of on-line social networks in the European Union, including Opinion 5/2009 from the Article 29 Working Group on the on-line social network.

22. After discussions, which covered a wide range of existing documents in this field, and also highlighted the impossibility of foreseeing the legal force of the prospective document, it was decided not to instigate any standard-setting work on on-line social networks. The subject did, however, deserve the T-PD's close attention, and it was therefore decided to continue exploring various pointers in close co-operation with the Steering Committee on the Media and New Information Services (CDMC).

23. It was decided that the proposed amendments to Convention 108 (item 1.1 of the Work Programme) would, for procedural reasons, be included in an additional protocol to this Convention. Priority was given to item 1.1.

24. It was also decided to prioritise the updating of Recommendation No. R (87) 15 regulating the use of personal data in the police sector. Drawing on the information received, the working group set up in the T-PD would prepare the preliminary draft to be subsequently presented at the Bureau and plenary meetings. After examination, if the T-PD saw fit, the regulations on the use of personal data in the police sector might be set out in a legally binding instrument.

25. It was also decided to give top priority to Recommendation (89) 2 on the protection of personal data used for employment purposes, in view of the need to update this document in the absence of harmonised regulations in this field.

26. In connection with item 3.5 (Preparation of the celebration of the 30<sup>th</sup> anniversary of the signature of Convention 108), the T-PD stressed that this event would be an opportunity for summarising the T-PD's previous work and initiating the debate on the future challenges to the protection of personal data.

27. It was decided to continue the work, where item 3.1 (status and competences of data protection supervisory bodies) was concerned, after judgment had been delivered in case no. C-518/07 before the Court of Justice of the European Communities, and, in connection with item 3.3 (Fundamental right to data protection), after the entry into force of the Treaty of Lisbon. The Steering Committee on Human Rights was added as another partner for the activity mentioned in item 3.3.

28. The T-PD adopted the document entitled "Work Programme for the T-PD for 2009 and beyond" as reproduced in Appendix III to this report.

## **VII. PRESENTATIONS**

29. The T-PD took note of the presentation by the European Privacy Association on its activities and structure, and noted its wish to obtain observer status with the T-PD. Once the Secretariat had received the request for observer status, it would be put to the vote of the T-PD, in pursuance of Article 4 bis of the Rules of Procedure.

30. The T-PD took note of the presentation of the work of the Group of Specialists on Predictivity, Genetic Testing and Insurance of the Steering Committee on Bioethics, and instructed the Secretariat to call for a T-PD member to participate in the work of this Group.

31. The T-PD took note of the presentation on the Expert Group on Anti-Doping and Data Protection of the Ad Hoc European Committee for the World Anti-Doping Agency (CAHAMA), and instructed Mr José Leandro Nuñez Garcia (Spain) to represent the T-PD at the next meeting of the aforementioned committee in Madrid on 14 September 2009.

## **VIII. DISCUSSION AND ADOPTION OF THE DECLARATION ON THE JOINT PROPOSAL FOR DRAFT INTERNATIONAL STANDARDS ON PROTECTION OF PRIVACY WITH REGARD TO PROCESSING OF PERSONAL DATA**

32. The T-PD discussed and approved the Declaration on the joint proposal for draft international standards on protection of privacy with regard to processing of personal data as reproduced in Appendix IV to this report. The Secretariat was instructed to transmit this Declaration to the secretariat of the International Conference of Data Protection and Privacy Commissioners.

## **IX. DATA PROTECTION DAY**

33. Ms Hana ŠTEPÁNKOVÁ (Czech Republic) presented the questionnaire which had been submitted to the T-PD by a working group set up in the International Conference of Data Protection and Privacy Commissioners, geared to establishing a day or a week, other than 28 January, to celebrate and promote data privacy and protection worldwide every year.

34. A number of delegations, as well as the European Commission representative, stressed that Data Protection Day had already been celebrated several times and that 28 January was becoming a familiar date across the Atlantic, with activities having been organised in the USA on that day the previous year.

35. It was decided that Data Protection Day should continue to be celebrated on 28 January, as proposed by the T-PD at its 22<sup>nd</sup> plenary session in 2006 and as decided by the Committee of Ministers of the Council of Europe (CM/Del/Dec(2006)962/10.1). It was agreed that the activities might be organised in the week surrounding this date, thus retaining some flexibility. Furthermore, this in no way prevented individual states from organising data protection awareness activities at other times.

## **X. INFORMATION ON 2009 DATA PROTECTION DAY AND MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD SINCE THE 24<sup>th</sup> T-PD MEETING (13 and 14 March 2008)**

35. The T-PD held a brief exchange of information on national developments in the data protection field.

36. It also invited all delegations to send their information on national developments in the data protection field to the Secretariat so that they could be included in Appendix IX to this report.

## **XI. DATA OF THE NEXT PLENARY SESSION**

37. The T-PD took note of the date of the next plenary meeting, to be held in Strasbourg from 1 to 3 June 2010.

## APPENDIX I - AGENDA

### 1. OPENING OF THE MEETING

### 2. ADOPTION OF THE AGENDA

### 3. STATEMENT BY THE SECRETARIAT

- T-PD (2008) RAP 24 Report of the 24<sup>th</sup> 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] (13-14 March 2008)
- T-PD-BUR (2008) RAP 14 Report of the 14<sup>th</sup> meeting of the T-PD-BUR (Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] – (10-11 June 2008)
- T-PD-BUR (2008) RAP15 Report of the 15<sup>th</sup> meeting of the T-PD-BUR (13-14 October 2008)
- T-PD-BUR (2008) RAP16 Report of the 16<sup>th</sup> meeting of the T-PD-BUR (17-18 December 2008)
- T-PD-BUR (2009) RAP17 Report of the 17<sup>th</sup> meeting of the T-PD-BUR (9-10 February 2009)
- T-PD-BUR (2009) RAP18 Report of the 18<sup>th</sup> meeting of the T-PD-BUR (6-7 July 2009)

### 4. ELECTION OF THREE BUREAU MEMBERS

### 5. 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, in view of the contributions received*

- T-PD (2008) 1 Final version of the study on the application of Convention 108 to the profiling mechanisms
- T-PD-BUR (2009) 5 Revised table containing the draft recommendation on the protection of individuals with regard to automatic processing of personal data used in the framework of profiling and as resulting from the 18<sup>th</sup> Bureau meeting (6-7 July 2009)



- T-PD-BUR(2009)2 Rev 3 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 18<sup>th</sup> Bureau meeting (6-7 July 2009)
- T-PD-BUR(2009)6 MOS Comments on 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(2009)6 ENG

#### 6. T-PD'S FUTURE ACTIVITIES

*Required action: the T-PD will be called upon to discuss and approve its work programme for the coming years*

- T-PD (2009) 3 Draft work programme for the T-PD as resulting from the 18<sup>th</sup> Bureau meeting (6-7 July 2009)

#### 7. DISCUSSION OF THE JOINT PROPOSAL FOR A DRAFT OF INTERNATIONAL STANDARDS ON THE PROTECTION OF PRIVACY WITH REGARD TO THE PROCESSING OF PERSONAL DATA

*Required action: the T-PD will be called upon to adopt the statement on the Draft Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data*

- T-PD (2009) 4 Statement on the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data

#### 8. PRESENTATION BY:

The Ad hoc European Committee for the World Anti-Doping Agency (CAHAMA) on the "WADA International Standard for the Protection of Privacy and Personal Information" and on the participation of the T-PD in the Cahama Working Party on anti-doping and data protection issues

CM - 1018th meeting  
20 February 2008  
Appendix 14 (Item 8.2) Terms of reference of the Ad hoc European Committee for the World Anti-Doping Agency (CAHAMA)

- T-PD-BUR (2008) 04 fin Draft Opinion of the T-PD on the Compatibility of the World Anti Doping Agency's International Standard for the Protection of Privacy and Personal Information with the Council of Europe Data Protection Standards

The Group of specialists on predictivity, genetic testing and insurance of the CoE's Steering Committee on Bioethics

Terms of reference of the Group of Specialists on Human Genetics (CDBI-CO-GT4)

Explanatory note concerning the work of the Group of specialists on predictivity, genetic testing and insurance

The European Privacy Association

Document presenting the European Privacy Association

9. DATA INFORMATION ON THE 2009 DATA PROTECTION DAY AND ON MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD SINCE THE 24<sup>TH</sup> MEETING OF THE T-PD (13-14 MARCH 2008)

*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 15<sup>th</sup> of August.*

- DPD (2009) Compilation      Compilation of the participation forms received for the 2009 Data Protection Day
- T-PD (2009) 5 mos            Information on recent developments at national level in the data protection field

10. DATE OF THE 26<sup>TH</sup> PLENARY MEETING OF THE T-PD IN 2010

## APPENDIX II – LIST OF PARTICIPANTS

### MEMBERS OF THE T-PD

#### **ALBANIE/ALBANIA**

---

Flora Çabej Pogaçe, Albanian Commissioner for Personal Data Protection

Erton Karagjozi, Director of the Registration Department, Commissioner for Personal Data Protection

#### **ANDORRA/ANDORRE**

---

Florencia Aleix, Représentante permanente adjointe de l'Andorre auprès du Conseil de l'Europe

#### **AUSTRIA/AUTRICHE**

---

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

#### **BELGIUM/BELGIQUE**

---

Joëlle Jouret, SPF Justice, Direction générale de la législation et des libertés et droits fondamentaux, Service des droits de l'homme

#### **BOSNIA AND HERZEGOVINA / BOSNIE HERZEGOVINE**

---

Samira Campara, Director Assistant, Agency for personal data protection

Selma Maksumic, Assistant, Agency for personal data protection

#### **CROATIA/CROATIE**

---

Vilena Gašparović, Deputy Director, Croatian Personal Data Protection Agency

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

#### **CYPRUS/CHYPRE**

---

Nonie Avraam, Office of the Commissioner for personal data protection

#### **CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE**

---

Hana Štěpánková, Head of the Press Department, Spokeswoman, Office for Personal Data Protection

#### **DENMARK/DANEMARK**

---

Astrid Gade, Head of Section, Datatilsynet

#### **ESTONIA/ESTONIE**

---

Kaja Puusepp, Supervision Director, Estonian Data Protection Inspectorate

#### **FINLAND/FINLANDE**

---

Leena Rantalankila, Ministerial Adviser, Ministry of Justice

**FRANCE**

---

Mme Catherine Pozzo di Borgo, Commissaire du Gouvernement adjoint auprès de la CNIL, Services du Premier Ministre

**GERMANY/ALLEMAGNE**

---

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

**GEORGIA/GEORGIE**

---

Giorgi Jokhadze, Head of Analytical Department, Ministry of Justice

**HUNGARY/HONGRIE**

---

Kinga Szurday, Senior legal counsellor, Ministry of Justice and law enforcement

**IRELAND/IRLANDE**

---

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

**ITALY/ITALIE**

---

Alessandra Pierucci, Civil Servant at the Italian Data Protection Authority, Garante per la Protezione dei Dati Personali

**LATVIA/LETTONIE**

---

Signe Plumina, Director, Data State Inspectorate of Latvia

Aiga Balode, Deputy Director, Data State Inspectorate of Latvia

**LITHUANIA/LITUANIE**

---

Rita Vaitkevičienė, Deputy Director, State Data Protection Inspectorate

**LIECHTENSTEIN**

---

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

**LUXEMBOURG**

---

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

**MALTA/MALTE**

---

Ingrid Camilleri B.A., Head of Legal Unit, Office of the Data Protection Commissioner

**MOLDOVA**

---

Valentina Popovici, Deputy Director of the Scientific Research and Analysis Division of the Ministry of Informational Technologies

**NETHERLANDS/PAYS-BAS**

---

Excused/excusé

**NORWAY/NORVEGE**

---

Birgitte Istad, Adviser, Ministry of Justice

**POLAND/POLOGNE**

---

Urszula Góral, Director, Social Education and International Cooperation Department, Bureau of the Inspector General for Personal Data Protection

**PORTUGAL**

---

Joao Pedro Cabral, [*Chair of the T-PD*], Directorate General of Justice Policy, Ministry of Justice

Excusé/excused

Cláudia Maduro Redinha , Directorate General of Justice Policy, Ministry of Justice

**ROMANIA/ROUMANIE**

---

Georgeta Basarabescu, President of the National Supervisory Authority for Personal Data Processing

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

**SERBIA/SERBIE**

---

Nevena Ruzic, Commissioner for Information of Public Importance and Personal Data Protection, Head of the Office

**SLOVAKIA/SLOVAQUIE**

---

Veronika Žuffová–Kunčová, State Counselor, Foreign Relations Department, Personal Data Protection Office of the SR

**SLOVENIA/SLOVENIE**

---

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

**SPAIN/ESPAGNE**

---

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

**SWEDEN/SUEDE**

---

Eva Lenberg, Director, Ministry of Justice

David Törngren, Legal Adviser, Ministry of Justice

**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

**“THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA” / « L’EX-RÉPUBLIQUE YUGOSLAVE DE MACÉDOINE »:**

---

Marijana Marusic, Director, Directorate for Personal Data Protection

**UNITED KINGDOM/ROYAUME-UNI**

---

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

## **SCIENTIFIC EXPERTS**

Yves Pouillet, Directeur du CRID (Centre de Recherches Informatique et Droit), Faculté de Droit

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

## **COMMISSION OF THE EUROPEAN COMMUNITIES**

Hana Pecháčková, Directorate General Justice, Freedom and Security, D5 Data Protection Unit,

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

## **OBSERVERS**

### **MEXICO / MEXIQUE**

---

María Marván Laborde, Commissioner of the Federal Institute of Access to Public Information (IFAI) of Mexico

### **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

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

---

Christopher Kuner, Hunton & Williams, Park Atrium

### **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,

### **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,

## **INVITED**

### **EUROPEAN PRIVACY ASSOCIATION**

---

Karin Riis-Jorgensen, Chairwoman and Funder of the European Privacy Association

## **SECRETARIAT**

### **DIRECTORATE GENERAL OF HUMAN RIGHTS AND LEGAL AFFAIRS**

#### **Directorate of Standard-Setting**

##### **Law reform Department**

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

- **Public and Private Law Division**

##### ***Data Protection***

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**

- **Media and Information Society Division**

Lee Hibbard, Administrator / Administrateur

Franziska Klopfer, Administrator / Administrateur

### **DIRECTORATE GENERAL III – SOCIAL COHESION**

#### **Bioethics Division**

Laurence Lwoff, Head of Division/Chef de la Division

Aysegül Elveris, Administrator/Administrateur

### **DIRECTORATE GENERAL OF EDUCATION, CULTURE AND HERITAGE, YOUTH AND SPORT**

#### **Sport Department**

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

### **INTERPRETERS**

Cynera JAFFREY  
Nicolas GUITTONNEAU  
Christine TRAPP-GILL

## APPENDIX III – WORK PROGRAMME FOR THE T-PD FOR 2009 AND BEYOND

As approved by the T-PD at the 25<sup>th</sup> plenary meeting

### WORK PROGRAMME FOR THE T-PD FOR 2009 AND BEYOND

#### 1 Amendments to the Convention 108<sup>1</sup>

Following the example of the Additional Protocol (ETS No. 181), several amendments concerning the different topics could be treated simultaneously. In this context the priorities should be identified among the topics proposed in this chapter.

##### 1.1 *Convention 108 and technological developments*

**Objective:** to evaluate the need for additional regulatory provisions that are necessary to meet the challenges to data protection posed by technological developments (Internet etc.)

##### 1.2 *Automated individual decisions*

**Objective:** to add provision regarding the automated individual decisions

##### 1.3 *Information that needs to be provided to the data subject by the controller*

**Objective:** to add provision defining the information which shall be provided by the controller to the data subject on the processing of his/her personal data

##### 1.4 *Monitoring the implementation of the Convention by 108 Contracting States*

**Objective:** to invest the Consultative Committee with the power of monitoring the implementation of Convention 108 and its Additional Protocol by Member States and, eventually, to evaluate the level of protection of personal data of the State candidates for accession to Convention 108 and its Additional Protocol

<sup>1</sup> Activities carried out according to Article 21 of Convention 108



**Working methods:** the T-PD will consider the setting up of several working groups in charge of selected issues. These working groups, coordinated by a rapporteur (a member of the T-PD), will be composed of members of the T-PD and other representatives of the Contracting Parties, observer organisations and States. The groups must be large enough to provide the necessary expertise but not that large to hinder the effectiveness of work. Participation of experts may be considered provided that sufficient funding is available. The groups will work via email. The draft amendments will be discussed at the Bureau meetings in presence of the rapporteurs of the groups concerned. The Secretariat will prepare the document which will incorporate the proposed amendments and provide the preliminary Draft of the Additional Protocol.

**Partner (s):** CRID, CoE experts

**Calendar:** The first draft of the Additional Protocol could be prepared for the plenary meeting in 2012.

**Rank of priorities:** [Top](#)

## 2 Revision of "old" and drafting of "new" Recommendations<sup>2</sup>

### 2.1 Recommendation No. R (87) 15 regulating the use of personal data in the police sector

**Objective:** the development of new concepts and techniques for processing of personal data necessary for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties calls for the revision of the Recommendation (87) 15 or for the drafting of a new legally binding instrument.

**Working methods:** the T-PD will initiate a study of Recommendation (87) 15 to determine the principles to be developed in order to cover adequately the emerging issues of data protection in the field of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The possibility of submitting a questionnaire on domestic legislation and practice to the Contracting States may be considered. On the basis of information received, the working group established within the T-PD will be responsible for the preparation of the preliminary draft, subject to further discussion at the Bureau and plenary meetings. After evaluation, if the T-PD deems this necessary, the regulation of the use of personal data on the police sector could be a subject of a legally binding instrument.

**Partner (s):** CoE experts, European Data Protection Authorities

**Calendar:** 2 years, the first draft can be submitted at the plenary in 2012

**Rank of priorities:** [Top](#)

---

<sup>2</sup> To carry out the activities mentioned in this chapter, a prior mandate shall be received from the CDCJ.

## **2.2 Recommendation No. R (89) 2 on the protection of personal data used for employment purposes**

**Objective:** to update Recommendation (89) 2 in light of technological developments as well as of other texts of the Council of Europe containing provisions on the processing of data in the employment field.

**Working methods:** the T-PD will initiate a study of Recommendation (89) 2 to determine the principles to be developed in order to cover adequately the emerging issues of data protection in the employment field. The possibility of submitting a questionnaire on domestic legislation and practice to the Contracting Parties may be considered. On the basis of information received, the working group established within the T-PD will be responsible for the preparation of the preliminary draft, subject to further discussion at the Bureau and plenary meetings.

**Partner (s):** CoE experts, the Secretariat of the European Social Charter

**Calendar:** 2 years, the first draft can be submitted at the plenary in 2014

**Rank of priorities:** [Top](#)

### **3. Other work**

#### **3.1 Status and powers of data protection supervisory authorities**

**Objective:** to draft an explanatory document setting out a "model" of the supervisory authority as foreseen by the Additional Protocol.

**Working methods:** firstly, the Bureau and the T-PD will develop a questionnaire dealing with the organisation and competences of supervisory authorities and distribute it to the Contracting Parties. The Bureau will then prepare a compilation document outlining a "model" to accompany the implementation of the Additional Protocol.

**Partner (s):**

**Calendar:** activity to be pursued after the judgment of the Court of Justice of the European Communities (ECJ) in case C-518/07.

#### **3.2 Online social networking**

**Objective:** to prepare a study taking into account existing instruments aiming at strengthening the rights of users in the context of the expanding phenomenon of online social networking

**Working methods:** the T-PD, in collaboration with representatives of the CDCJ as well as the Steering Committee on the Media and New Communication Services (CDMC), will explore the ideas concerning the working methods and the funding of the work on the draft recommendation.

**Partner (s):** CDMC, experts Coe

**Rank of priorities:** [Secondary](#)

### 3.3 Fundamental right to data protection

**Objective:** to carry out a study in order to assess the need and added value of a fundamental right to data protection, distinct of Article 8 of the ECHR

**Partner (s):** Steering committee on human rights (CDDH)

**Calendar:** activity to be pursued after the Lisbon Treaty enters into force

### 3.4 *Opinions on the compatibility with the Council's of Europe data protection instruments*

**Objective:** the constant follow-up of developments within and outside the Council of Europe with data protection instruments of the Council of Europe.

**Working methods:** the Secretariat of the T-PD will be responsible for constantly updating the documents "Council of Europe achievements in the field of data protection" and "The case-law of the European Court of Human Rights concerning the protection of personal data"

**Partner (s):** Secretariat of the T-PD

**Rank of priorities:** constant issue

### 3.5 *Preparation of the celebration of the 30th anniversary of signature of the Convention 108*

**Objective:** gather proposals with the view to organising the trans-border celebration of the 30<sup>th</sup> anniversary of signature of the Convention 108

**Working methods:** The Bureau will prepare a questionnaire to be submitted to Member States. The compilation of proposals, prepared by the Secretariat, will be discussed during the plenary meeting with the view to adopting of the common plan of action.

**Calendar:** Questionnaire to be approved during the Bureau meeting on 19-20 November 2009/ the common plan of action to be discussed during the 2010 plenary meeting.

**Partner (s):** Secretariat of the T-PD

**Rank of priorities:** constant issue

# **APPENDIX IV - STATEMENT ON THE JOINT PROPOSAL FOR A DRAFT OF INTERNATIONAL STANDARDS ON THE PROTECTION OF PRIVACY WITH REGARD TO THE PROCESSING OF PERSONAL DATA**

**As adopted by the T-PD at the 25th plenary meeting**

## **Introduction**

As the forum for policy-making and standard-setting under the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter Convention 108), the Consultative Committee of the Convention 108 (T-PD) would like to formulate the following observations on the “Joint proposal for a draft of international standards on the protection of Privacy with regard to the processing of personal data” (hereafter “draft international standards”).

The draft international standards were prepared by a working group coordinated by Spanish Data Protection Authority for the International Conference of Data Protection and Privacy Commissioners, following Montreux Declaration (2005) and Strasbourg Resolution (2008).

At its 25th meeting, held from 2 to 4 September 2009 in Strasbourg, the T-PD examined the draft international standards discussed at the meeting of the working group held on 11 June in Bilbao.

It is expected that the International Conference of Data Protection and Privacy Commissioners ascertains the draft international standards at their forthcoming conference in Madrid (4-6 November 2009).

## **General comments on the relationship between the international standards and Convention 108**

The declared purpose of the draft international standards is to define a set of principles and rights guaranteeing the effective protection of privacy with regard to the processing of personal data with a view to facilitating international flows of personal data.

The T-PD welcomes this attempt to provide an up-to-date statement of the applicable principles. Such an endeavour is particularly important and timely in an increasingly globalised world characterised by rapid technological development which transforms the communication between individuals and public and private organisations.

The T-PD notes that the draft international standards took Convention 108 and its Additional Protocol as one of their sources. This is only consequent, taking into account that Convention 108 and its Protocol remain for the time being the only legally binding international standard which has the potential to be applied worldwide. Being drafted in a simple and technologically-neutral way, the fundamental standards contained in Convention 108 remain valid. Its strengths are its legally binding force and its cross-cutting scope of application. Convention 108 protects against privacy intrusions by public and private authorities, regardless the ways of automatic processing.

The Council of Europe's Committee of Ministers adopted on 2 July 2008 a decision encouraging the accession of non member States with the required data protection legislation. This decision followed similar calls from European and International privacy and data protection authorities, in particular, the call launched by the Commissioners in Montreux Declaration. The T-PD counts on continued support by the International Conference of Data Protection and Privacy Commissioners in that important endeavor as well as on its active involvement in the T-PD activities as an observer.

The draft international standards are a set of principles, which provide guidelines for national legislation. They may in particular be used to assess the compatibility of national legal frameworks for the purpose of ensuring the free flow of personal data.

The draft international standards may help to interpret some of the provisions of Convention 108 in the light of modern technological developments or even to develop them through the adoption of new legal instruments, such as Committee of Ministers' recommendations, guidelines or even Additional Protocols to Convention 108.

It could lead to a new impetus contributing to the strengthening of data protection worldwide. The adoption of an up-to-date set of principles on data protection and privacy could thereby contribute to the worldwide promotion of Convention 108 and its additional Protocol. In this way, the much called-for harmonisation and a reinforcement of the global nature of the right to privacy and personal data protection would be ensured.

# APPENDIX V - EUROPEAN PRIVACY ASSOCIATION PRESENTATION

## Mission

---

The **European Privacy Association (EPA)** is a non-party-political pan-European network of privacy, data protection and security experts based in Brussels, Belgium. Its aim is to provide a 'space' for bringing together experts from across Europe, to engage with them as we seek out new policies to enhance privacy, e-security and data protection. EPA will work closely with European institutions, particularly the European Parliament, academia, civil society, and industry. EPA will engage with policy makers, industry, advocates, and the media, to bring forward new ideas and to propose policy frameworks to deal with pressing privacy issues as they arise. EPA will therefore be a clearinghouse for new ideas on preserving and enhancing privacy protection across Europe.

EPA is a forum dedicated to ensure the rule of law for the processing of personal data in the global information economy and society. EPA involves not only the best European specialists in privacy law, but also representatives of the public and private spheres, who often deal with personal data and sensitive information on a daily basis. Working as a think tank, EPA aims to consolidate itself as a meeting place for European "new law" experts, and for several of the players of high technology content markets, including industries and policy makers. EPA will be the first independent cross-sector organization dealing with privacy and security issues at the European level.

The European Privacy Association is led by an administrative council (Executive Board) with functions of management and direction, co-operating with a Scientific Committee that is composed of scholars, advocates, and experts on the subject of privacy. These groups are assisted in turn by a Committee of Supporters, comprised mostly of companies tasked with direct financing and fund-raising. EPA shall gather some of the most prominent experts in the security and data protection field, including law scholars, law firms' representatives, experts on new media and communication, market and competition, and professionals or academics in the areas of sociology, psychology and international politics.

## Objecives

---

- EPA shall bring together policy makers with experts from academia, civil society, and industry to provide insight into leading research and innovations relating to privacy and data protection.
- EPA aims to develop and provide new privacy and data protection policies to public officials and elected members at European and Member State level.
- EPA shall consult policy makers and industries on issues regarding personal data and security.
- Industries shall view EPA as an advisory organisation regarding current and future topics in the privacy and data protection field. EPA aims to help the market evolve by developing the correct strategies concerning privacy and security.
- EPA shall provide studies and analysis that envisage the future in the privacy field, favouring the proactive development of new policies and the rapid adaptation of the market.
- EPA shall promote advanced training seminars on privacy issues for European professionals.

- EPA shall recognise and award the best practices in the privacy and security field.
- EPA shall act as a watchdog to monitor the use of personal data and security measures by industries, institutions and authorities.

---

**Primary areas of interest**

---

- Privacy, international security and anti-terrorism
- Privacy and human rights
- E-Government and protection of citizens' data
- Internet advertising and other forms of consumer profiling
- Identity management and identity assurance
- Cybersecurity
- Search engines and social networks
- Intellectual property rights, anti-piracy and users' e-privacy
- Privacy and e-health systems
- Privacy and innovation
- Justice, e-crimes and anti-phishing

**Special focus to the Internet and converging media**

---

EPA works to ensure that European Internet users are properly protected against invasions of their personal privacy. EPA conducts analyses and formulates policy proposals based on the following principles:

Privacy is a basic human right. Without privacy, citizens are not fully free to search for information, conduct business, and participate in the public debate online.

The Internet industry (i.e. service providers, search engines, and others) has a responsibility to ensure the privacy of their customers.

Governments have a responsibility to ensure the privacy of its citizens, including properly safeguarding personal information in public databases. Governments should not be able to infringe on privacy without proper cause and due process.

EPA believes that privacy is best protected when citizens all over the European Union work together to hold governments and the industry accountable. EPA therefore actively cooperates with individuals and groups in other European countries who share our mission and principles.

## Types of activities

---

As its principle working tool, EPA uses its website (in the role of “electronic magazine”), to which its fellow partners and other researchers may contribute with publications, and a semi-monthly informative newsletter, which provides major news and analysis on the evolution of privacy issues in EU and the world. There will be meeting of the experts group every six months, as well as seminars run on a quarterly basis to brief policy-makers on the current pressing challenges and leading research, in partnership with European industries. This is done to improve training for professionals and to heighten the awareness of across sectors. The seminars will be broadcast over the internet, through EPA's portal, and are made available as downloadable or streamed content.

## Media Outreach

---

Among other activities, we will produce articles and other types of interventions for different media-partners (newspapers, magazines, TV, radio, web). In addition, the EPA will offer whitepapers and other publications on privacy. On a biannual basis, scholarships on the subject of ICT law will be awarded, according to the criteria established by the Scientific Committee and based on the economic resources made available by each business concerned.

## European Data Protection Award

---

Every year, beginning on January 28<sup>th</sup> 2010, Data Protection Day, EPA will award best privacy practice and research in the European context. Industries, campaigns and scholars will be recognised and rewarded for their work during the year in the privacy and data protection field.

## EPA Executive Board

---

The Executive board is comprised of a broad range of renowned experts in their own right:

**Karin Riis-Jørgensen (Chair)**, former Member of the European Parliament and Vice-President of the Liberal Group.

**Pat Cox (Vice-Chair)**, President of the European Movement International and former President of the European Parliament.

**Pietro Paganini PhD, (Executive Officer)**, Adjunct Professor at John Cabot University and independent consultant on innovation, market and competitiveness.

**Luca Bolognini** is the Chair of the Italian Institute for Privacy, and consultant for e-business, privacy, and new technologies laws in Italy.

**Birgitte Kofod Olsen (Treasurer)** is a human rights expert and former Vice Director of the Danish Institute for Human Rights. Ms Kofod Olsen is also member of the Danish IT Security Committee.

**Christopher Kuner** is a Partner of international law firm Hunton & Williams, Chair of the International Chamber of Commerce (ICC) Task Force on Privacy and Data Protection, and previously a member of the former Data Protection Expert Group of the European Commission.

**Gus Hosein** is an academic, a consultant, and an advocate. He is the Policy Director at Privacy International.



## Learn more about EPA

---

The European Privacy Association website ([www.europeanprivacy.eu](http://www.europeanprivacy.eu)) contains information more information on the backgrounds of the Executive Board and the profiles of our Scientific Committee members who span Europe and domains of expertise and interest. Also published online are all EPA press-releases, general news and membership details.

---

## APPENDIX VI - CETS No.: 108 – State of signatories and ratifications

### Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 108

Treaty open for signature by the member States and for accession by non-member States

#### Opening for signature

Place: Strasbourg  
Date : 28/1/1981

#### Entry into force

Conditions: 5 Ratifications.  
Date : 1/10/1985

Status as of: 22/9/2009

Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
<b>Albania</b>	9/6/2004	14/2/2005	1/6/2005	44		X	X			
Andorra	31/5/2007	6/5/2008	1/9/2008			X	X			
Armenia										
Austria	28/1/1981	30/3/1988	1/7/1988	44		X	X			
Azerbaijan										
Belgium	7/5/1982	28/5/1993	1/9/1993	44		X	X			
Bosnia and Herzegovina	2/3/2004	31/3/2006	1/7/2006							
Bulgaria	2/6/1998	18/9/2002	1/1/2003							
Croatia	5/6/2003	21/6/2005	1/10/2005	44		X	X			
Cyprus	25/7/1986	21/2/2002	1/6/2002	44			X			
Czech Republic	8/9/2000	9/7/2001	1/11/2001	44			X			
Denmark	28/1/1981	23/10/1989	1/2/1990	44			X	X		
Estonia	24/1/2000	14/11/2001	1/3/2002	44		X	X			
Finland	10/4/1991	2/12/1991	1/4/1992	44			X			
France	28/1/1981	24/3/1983	1/10/1985	44		X	X			
Georgia	21/11/2001	14/12/2005	1/4/2006	44						
Germany	28/1/1981	19/6/1985	1/10/1985	44		X	X	X		
Greece	17/2/1983	11/8/1995	1/12/1995	44						
Hungary	13/5/1993	8/10/1997	1/2/1998	44		X	X			
Iceland	27/9/1982	25/3/1991	1/7/1991	44			X			
Ireland	18/12/1986	25/4/1990	1/8/1990	44		X	X			
Italy	2/2/1983	29/3/1997	1/7/1997	44		X	X			
Latvia	31/10/2000	30/5/2001	1/9/2001	44		X	X			
Liechtenstein	2/3/2004	11/5/2004	1/9/2004	44		X	X			
Lithuania	11/2/2000	1/6/2001	1/10/2001	44			X			
Luxembourg	28/1/1981	10/2/1988	1/6/1988	44		X	X			
Malta	15/1/2003	28/2/2003	1/6/2003							
Moldova	4/5/1998	28/2/2008	1/6/2008			X	X			
Monaco	1/10/2008	24/12/2008	1/4/2009	44			X			
Montenegro	6/9/2005	6/9/2005	6/6/2006	56						

Netherlands	21/1/1988	24/8/1993	1/12/1993	44		X	X	X		
Norway	13/3/1981	20/2/1984	1/10/1985	44		X	X	X		
Poland	21/4/1999	23/5/2002	1/9/2002	44						
Portugal	14/5/1981	2/9/1993	1/1/1994	44			X			
Romania	18/3/1997	27/2/2002	1/6/2002			X	X			
Russia	7/11/2001									
San Marino										
Serbia	6/9/2005	6/9/2005	1/1/2006	44		X	X			
Slovakia	14/4/2000	13/9/2000	1/1/2001	44			X			
Slovenia	23/11/1993	27/5/1994	1/9/1994				X			
Spain	28/1/1982	31/1/1984	1/10/1985			X	X			
Sweden	28/1/1981	29/9/1982	1/10/1985	44			X			
Switzerland	2/10/1997	2/10/1997	1/2/1998	44		X	X			
the former Yugoslav Republic of Macedonia	24/3/2006	24/3/2006	1/7/2006			X	X			
Turkey	28/1/1981									
Ukraine	29/8/2005									
United Kingdom	14/5/1981	26/8/1987	1/12/1987	44		X	X	X		

#### Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
--------	-----------	--------------	------------------	-------	----	----	----	----	----	----

Total number of signatures not followed by ratifications:	3
Total number of ratifications/accessions:	41

#### Notes:

(44) Party having accepted the amendments of 15th June 1999 allowing the European Communities to accede to this Convention.

(56) Dates of signature and ratification by the state union of Serbia and Montenegro.

a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".

R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

Source : Treaty Office on <http://conventions.coe.int>

## APPENDIX VII - CETS No.: 181 – State of signatories and ratifications

**Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows**  
**CETS No.: 181**

Treaty open for signature by the Signatories of the treaty ETS 108 and by the European Union, and for accession by the States having acceded to treaty ETS 108

**Opening for signature**

Place: Strasbourg  
Date : 8/11/2001

**Entry into force**

Conditions: 5 Ratifications.  
Date : 1/7/2004

**Status as of: 9/2/2010**

Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	9/6/2004	14/2/2005	1/6/2005							
Andorra	31/5/2007	6/5/2008	1/9/2008				X			
Armenia										
Austria	8/11/2001	4/4/2008	1/8/2008							
Azerbaijan										
Belgium	30/4/2002									
Bosnia and Herzegovina	2/3/2004	31/3/2006	1/7/2006							
Bulgaria										
Croatia	5/6/2003	21/6/2005	1/10/2005							
Cyprus	3/10/2002	17/3/2004	1/7/2004							
Czech Republic	10/4/2002	24/9/2003	1/7/2004							
Denmark	8/11/2001									
Estonia	15/12/2008	28/7/2009	1/11/2009							
Finland	8/11/2001									
France	8/11/2001	22/5/2007	1/9/2007							
Georgia										
Germany	8/11/2001	12/3/2003	1/7/2004			X				
Greece	8/11/2001									
Hungary	30/3/2004	4/5/2005	1/9/2005							
Iceland	8/11/2001									
Ireland	8/11/2001	5/5/2009	1/9/2009							
Italy	8/11/2001									
Latvia	22/5/2007	21/11/2007	1/3/2008							
Liechtenstein	28/1/2010	28/1/2010	1/5/2010							
Lithuania	8/11/2001	2/3/2004	1/7/2004							
Luxembourg	24/2/2004	23/1/2007	1/5/2007							
Malta										
Moldova										
Monaco	1/10/2008	24/12/2008	1/4/2009							
Montenegro	24/2/2009									

Norway	8/11/2001																			
Poland	21/11/2002	12/7/2005	1/11/2005																	
Portugal	8/11/2001	11/1/2007	1/5/2007																	
Romania	13/7/2004	15/2/2006	1/6/2006																	
Russia	13/3/2006																			
San Marino																				
Serbia	2/7/2008	8/12/2008	1/4/2009																	
Slovakia	8/11/2001	24/7/2002	1/7/2004																	
Slovenia																				
Spain	24/9/2009																			
Sweden	8/11/2001	8/11/2001	1/7/2004																	
Switzerland	17/10/2002	20/12/2007	1/4/2008																	
The former Yugoslav Republic of Macedonia	4/1/2008	26/9/2008	1/1/2009																	
Turkey	8/11/2001																			
Ukraine	29/8/2005																			
United Kingdom	8/11/2001																		X	

Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
--------	-----------	--------------	------------------	-------	----	----	----	----	----	----

International Organisations

Organisations	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
---------------	-----------	--------------	------------------	-------	----	----	----	----	----	----

Total number of signatures not followed by ratifications:	13
Total number of ratifications/accessions:	26

**Notes:**

a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".  
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

## **APPENDIX VIII - INFORMATION ON RECENT DEVELOPMENTS AT NATIONAL LEVEL IN THE DATA PROTECTION FIELD**

### **ALBANIA**

Albania is among those countries which have ratified the Convention for the protection of individuals with regard to automatic processing of personal data (Council of Europe, ETS 108, 1981) and the Additional Protocol to the Convention 108.

One of the requirements and important priorities of our Country when signing the Association and Stabilization Agreement was to set up of the Authority responsible for monitoring the data protection. This Authority is independent and exercises the legal competences pursuant to law no.9887, dated 10/03/2008 "on the protection of personal data".

The above mentioned law is in accordance with all the requirements of the Directive 95/46/EC, the best international practices and the Albanian Constitution and, as a consequence, guarantees an adequate level of data protection.

Also, based on the Law nr.8792, dated 10.05.2001 "on the establishment of the Center for Data Processing in the State Police", it has been established "the Center for data protection and processing in the police sector", which depends on the General Department of the State Police. By achieving all this Albania is currently considered as a country ensuring an adequate level of data protection.

Article 29 of the Law Nr. 9887, established the Commissioner For the Protection of Personal Data as the authority responsible for supervising and monitoring the protection of personal data by respecting and guaranteeing the fundamental human rights and freedoms in compliance with the law. The Commissioner for the Protection of Personal Data has the status of an independent public legal person.

The Chief of the Office, referred to as the Commissioner, was elected by the Assembly by decision no.211 dated 11.9.2008 and the internal structure or organization of the Office was approved by decision no.225, dated 13.9.2008.

Our office is organized into five departments:

- The department of notifications (central register).
- The department of procedural and legal matters and foreign relations.
- The department of inspection.
- The department of public relations.
- The department of support services.

## **1. The issuing of several legal documents prepared in order to efficiently implement the law.**

Since the establishment of the Office several documents have been prepared in order to perform our work with efficiency and responsibility and different activities have been organised in the framework of staff training and the awareness of the public and private bodies about the importance of the implementation of the law and the functioning of the Office.

Several documents have been issued to this date; our office has adopted the institution's ethical code of conduct and the internal regulation which determines in details the specific tasks and responsibilities of each department.

We have issued also a commentary on the law which is very useful to better explain and understand the text.

In accordance with the Law on the protection of personal data we have prepared two decisions of the Council of Ministers. The first relates to the list of countries having an adequate level of data protection. The second relates to the exemptions from notifications.

Currently we are preparing the notification form and its guidelines which are yet to be approved.

During the month of April 2009 in compliance with the Law on the protection of personal data we compiled and send the first activity report to the Assembly.

## **2. Awareness of the public and cooperation with other institutions.**

It is worth mentioning that Our Office and the Council of Europe have organized the fourth of July 2009 a conference on the Protection of Personal Data in Albania. Among the participants were government personalities and representatives of the EC and OSBE.

There have been close cooperation with important state institutions as for example the people's advocate, the center for data processing of the state police etc...

An important tool for making people aware of the importance of data protection is internet. Very soon our website will be available contain very useful materials and instructions for data subjects and data controllers. We are working hard about it.

In the future our website will be an additional opportunity for being more informed because of the updated functioning.

As a consequence of our work in this direction, we have received complaints from citizens related especially to problems with the civil registry and the social insurance institute.

## **3. Training**

Being a new institution and almost with no tradition in our country we consider training inside and outside the Country as indispensable. Since the establishing of the Office, part of our staff has attended three study visits in Portugal, Czech Republic and Croatia.

Also, in the framework of the Council of Europe project, our Office has been assisted by the English Expert of the CE Mr. Graham Sutton and currently by Mr. Karel Neuwirt (ex Czech Commissioner) for the drafting of the Law on data protection and the establishment of the Independent Institution. Their assistance has been very helpful to all of our staff for better performing our respective tasks with a higher expertise.

It is worth mentioning that this project is an extra budgetary source in addition to our own independent budget which is funded by the state budget in accordance with the article 38 of the Law 'On the protection of personal data'.

Finally, the Commissioner and part of our staff have organized a seminar in the City of Shkodra (Albania) attended by representatives of the Social Insurance Institute, Police Department, Civil Registry Office, Central Bank etc, where legal topics were addressed by analyzing the law on data protection and where took place discussions and the giving of opinions relating to the interest shown from the attendants in the new field but very important for the development of our society toward the great European family.

## **CROATIA**

### **I. Legal framework**

In the European integration process the Member States are obliged to fulfil two conditions in the domain of personal data protection:

1. to enact a national law on personal data protection and
2. to establish a public supervisory authority.

As a Candidate Country, following the promulgation of the Act on Personal Data Protection (in further text: the Act) in 2003, the Republic of Croatia has established the Croatian Personal Data Protection Agency (in further text: the Agency) in 2004 as a supervisory body.

The Croatian Act has been amended twice - in 2006 and 2008:

- *Act on Amendments to the Act on Personal Data Protection (Official Gazette No. 118/06)* - There was a need for further harmonisation of Article 13 of the Croatian Act on transborder data transfer with Articles 25 and 26 of the Directive 95/46/EC.

The principle of an "adequate level of protection" stands for a fundamental principle of transfer of personal data (Article 25 of Directive 95/46/EC) and is introduced in Article 13 of the Croatian Act. However, the mentioned regulation was too flexible. It was also necessary to prescribe criteria in accordance with those mentioned in Article 25, point 2 as well as in Article 26, point 2 of the Directive 95/46/EC. According to those criteria the state can approve the transfer of personal data to a country without an adequate level of protection, when a data controller offers sufficient guarantees for the protection of privacy and fundamental rights and freedoms of an individual.

- *Act on Amendments to the Act on Personal Data Protection (Official Gazette, No. 41/08)* - the amendments consist in the following: data controllers employing up to five employees and those who have appointed a data protection officer are not obliged to deliver notifications on personal data filing systems concerning their staff to the Central Register (maintained by the Agency). This obligation remains if those data are being transferred outside of the Republic of Croatia.



However, the Progress Report for 2008 submitted by the European Commission in the negotiation process of the Republic of Croatia for the *Chapter 23 - Judiciary and fundamental human rights* in the part concerning personal data protection emphasises a need for a full harmonisation of the Act with the Directive on personal data protection and with other instruments of the Council of Europe.

With respect to the Commission's Report the Agency shall create a new Act on Personal Data Protection and contribute to a full harmonisation with the aquis communautaire covering personal data protection within its IPA Project under the title *Strengthening of Capacities of the Croatian Personal Data Protection Agency*.

With engagement of experts in the IPA Project there should be enough time until the second half of 2010 to elaborate on specific solutions coming from the existing valid law, which were not proved to be the best until now and are related to inspection, data officers, delivery of records on personal data, penal regulations etc.

## **II. Engagement in the international arena**

In 2008 the Agency has become a full member and a partner of 2 international conferences: the Spring Conference of the European Data Protection Authorities and the International Conference of Data Protection and Privacy Commissioners.

- **Central and Eastern Data Protection Authorities (CEEDPA)**

The Agency took part in the 10th Meeting of the Central and Eastern Data Protection Authorities held in 2008 in Poland. At the Meeting the Agency has emphasized the upcoming strengthening of its supervisory competencies within the framework of the IPA Project, the co-operation with Eurjoust and its role in the preparation of the Schengen Action Plan.

- **Article 29 Data Protection Working Party**

The Agency took part at meetings of the Working Party from Article 29 of the Directive 95/46/EC (Article 29 Data Protection Working Party). It has contributed to the work of the Working Party related to the Code prepared by WADA (World Anti-Doping Agency) concerning the data retention period.

- **Francophone Conference**

As a full member the Agency took part at the second Francophone Conference held in October 2008 in Strasbourg.

The Agency satisfies all requirements set up in the contract with EUROJUST as well as all conditions and requirements from the contracts with other international bodies such as INTERPOL, SELEC etc.:

- **Interpol**

The Agency has a representative in terms of an expert in electronic processing of personal data, who participates in the Commission for control of Interpol files. Namely, the Agency follows up the implementation of measures for personal data protection in the information systems.

- **Eurojust**

The Agency participates in the project on implementation of the Agreement signed between the Republic of Croatia and Eurojust in Brussels on November 9th, 2007. The Croatian Law on Confirmation of this Agreement has entered into force on September 27th, 2008.

- **SELEC (Southeast European Law Enforcement Center)**

The Agency participates in the Working Group on preparation of the Convention on establishment of SELEC in harmonising of the text of the SELEC Convention concerning protection in collection and processing of personal data.

- **SIRENE Office**

Within the framework of an EU programme TAIEX (Technical Assistance Information Exchange Unit) has organised a study visit of the Agency to the SIRENE Office in Vienna, which operates within the *Bundeskriminalpolizei* (Federal Criminal Police). The subject of the study visit was *Supervision of the State Border*. The Agency had an opportunity to learn about the organisation and the work of the SIRENE Office. The representatives of the Agency have also learned about the work of an organisational unit of the Austrian Police at the Schwechat Airport, which conducts surveillance activities. The SIRENE Office organised presentations on the state border supervision, on the procedure with asyle requesting parties as well as on the VISION system concerning an automatic system for mutual consultation on visa requests. There were also presentations on collection, processing and transfer of personal data in the Schengen Information System (SIS I and SIS II).

### **III. IPA PROJECT**

The Agency has proposed and drafted a Project framework within the 2007 IPA Programme, component I under the title *Strengthening of Capacities of the Croatian Personal Data Protection Agency*, which has been approved by the European Commission.

In 2008 the activities having fulfilled design conditions were completed. All accreditation criteria have been satisfied and a self-assessment has been conducted. For the purposes of the work on the Project a special education for Agency's employees has been organised and Project documentation and internal act on information security have been elaborated. Local and regional self-administration was also trained in personal data protection issues via numerous seminars and workshops. Those activities have fulfilled pre-conditions for the realisation of the Project, which should start in 2009.

The Project consists of two components: the legal and the technical one.

Within the legal component related to personal data protection the Twinning Contract has been in the moment of elaboration of this Report enriched through additional activities for the purpose of a full harmonisation of the Act on Personal Data Protection with the Directive 95/46/EC, strengthening of the advisory and the supervisory role of the Agency, ensuring of an efficient co-operation with the state bodies (especially with the Ministry of Interior and the Ministry of Justice). The Agency will start an awareness raising campaign among Croatian citizens on the necessity and importance of personal data protection and privacy as one of fundamental human rights (e.g. publicity campaigns and seminar on personal data protection nationwide).

The technical component of the Project shall be completed throughout a supply of equipment for improvement of Agency's IT structure and business processes, as well as throughout implementation of an international standard for information security ISO 27001.

In the preparatory phase of the Project Agency's employees are being educated.

We believe that during this Project in two years' time the Agency together with top European experts in the field of personal data protection will achieve the highest standard in personal data protection.

#### **IV. INSPECTION ACTIVITIES**

The Agency conducts ex-officio inspections and inspection upon requests. In 2008 the Agency had 539 ex-officio cases and in relation to the year 2007 the number of the filed requests has increased up to 77,55%.

In the recent period the accent was put on the inspection in the most important sectors (telecommunications, health and social care, trade, science, education etc.), whereas inspections in other sectors were carried out upon requests and complaints of the citizens.

Regarding the situation in the Central Register there has been a decrease in the notification delivery up to 5%. The reason for that lies in the previously mentioned Act on Amendments to the Act on Personal Data Protection, which have entered into force on April 17th, 2008 (Official Gazette No. 41/08).

By introducing these exemptions from notification into the Act on Personal Data Protection the Act has been harmonised with Art. 18, Point 2 of the Directive 95/46/EC. The exemptions made an influence on the quality of the content of the Central Register, since up to now the data controllers have mostly delivered notifications on staff related data. The obligation to deliver notifications on personal data filing systems is still in force, while the quality of the inspection activities has been improved. Data protection officers, who have been assigned by data controllers, are now taking over a direct internal supervision over personal data processing, which ensures an additional data protection and co-operation with the Agency.

#### **V. Awareness rising**

In accordance with one of its main tasks in terms of personal data protection the Agency has organised all sorts of activities (seminars, round tables, workshops and contacts with the media) in order to raise awareness of the Croatian citizens and data controllers on the right to personal data protection.

- **European Data Protection Day (28th January)**

In 2008 the Agency has organised celebration of the second European Data Protection Day together with the association "Potrošač" ('The Consumer'). The Agency has presented the Act and practical personal data protection solutions. It has issued special brochures and created a short questionnaire to get a general overview on the awareness of the citizens of their right to personal data protection.

In 2009 the Agency has organised an Info-desk at the National and University Library in Zagreb, which was a big success due to a big number of visitors. Agency's experts were distributing the information material to the citizens and other interested parties and had direct discussions with them on the data protection issues. At the same time the Agency has organised an Open Door Day and together with the director has wellcomed every interested citizen or data controller in its premises. Both events were followed by the media (press, Radio, TV, Internet).

## **CYPRUS**

The Office of the Commissioner for Personal Data Protection has prepared a draft Amendment Law in order to be completely complied with the Directive 95/46 EC. The Amendment Law is not yet entered into force. This Amendment Law provides for new extended powers for the Commissioner in order to be able to exercise his powers more efficiently. When the new Law enters into force more details will be provided.

In 2008 the Commissioner issued a recommendation regarding the Ministry of Education and Culture's policy on educators' right to access their personal files.

The Commissioner issued an opinion regarding the processing of biometric data in the context of the employment sector and more specifically for monitoring employees' working hours. According to this opinion the collection and processing of employees' biometric data is not proportional to the above purpose and there for is in breach with the provisions of the data protection Law (proportionality principle). The opinion concludes that such processing is only permitted for purposes related to monitoring access to high security premises or regarding confidential filing systems.

## **FINLAND**

### **A. Implementation of Directives 95/46/EC and 2002/58/EC**

The Directive of the European Parliament, and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999. The Act was revised on 1 December 2000, when provisions on the Commission's decision-making, as well as how binding these decisions are in matters concerning the transfer of personal data to countries outside the Union under the Data Protection Directive were incorporated into it.

Protection of privacy has been a basic right in Finland since 1 August 1995. Under the Finnish Constitution, protection of personal data is regulated by a separate act.

The Act on Data Protection in Electronic Communications (516/2004), which entered into force on 1 September 2004, implemented the Directive on Privacy and Electronic Communications (2002/58/EC). The purpose of the law is to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications and the balanced development of a wide range of electronic communications services.

The responsibility for enforcing the law was divided between The Office of the Data Protection Ombudsman and the Finnish Communication Regulatory Authority. The mandate of the Office of the Data Protection Ombudsman includes: regulations on processing location data, direct marketing regulations, regulations on cataloguing services, and regulations on users' specific right to obtain information.

In this connection, it should be noted that according to the Penal Code, the prosecutor is obliged to consult the Data Protection Ombudsman before pressing charges in a matter concerning a violation of the secrecy of electronic communication.

## *Amendments*

During the year under review, there were no actual amendments to the Personal Data Act (523/1999) but provisions pertaining to personal credit data were extracted from it to form an Act in their own right. The transition period of the Credit Data Act ended on 1 November 2008. In part, the Act provides data protection also to legal persons and specifically requires that the data controllers have sufficient data protection competence at their disposal. A new chapter, 5a, was included in the Act on Protection of Privacy in Working Life, which provides detailed provisions on the use of personal credit data in working life.

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 deadline for their implementation will end on 15 March 2009.

In 2006, the Finnish Parliament demanded that the Government begin preparation of legislation on the general protection of personal data in biometric identification. The general provisions on the processing of biometric identification will be prepared in conjunction with the general review of the Personal Data Act (95/46/EC 8 art 7 paragraph) to be commenced later.

### **B. Major case law**

On 17 July 2008, the European Court of Human Rights gave its ruling in the matter of I vs Finland (no. 20511/03). The matter pertained, among other things, to a person's right to find out on the basis of log data who has had access to her patient records. The Finnish legislation requires taking care of data protection in part to specifically ensure that access to this kind of information can be ensured. However, the data system of the hospital was implemented in such a way that the administration of access rights and the log file could not indicate in detail the persons who had processed data on her. Due to this, and applying the principle of obligatory prosecution, the criminal court could not convict any one person of a crime. In its ruling, the European Court of Human Rights said that a situation has occurred, caused by functional characteristics of a data system that was not controlled as provided in the law, in which the protection of the personal life of the person in question as enacted in the Article 8 of the European Convention on Human Rights has been violated. The decision is particularly significant because the European Court of Human Rights applied the Convention on Human Rights to an electric data system and its deficiencies.

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 Court left the definition of the journalistic processing as referred to in Article 9 of Directive 95/46/EC to be done by a national court. On the other hand, according to the ruling, the Data Protection Directive must be applied to the processing of personal data derived from public data sources and the use of previously published lists or services. The matter is still being processed in the Supreme Administrative Court in Finland.

The competent Data Protection Board 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.

### **C. Specific issues**

#### *Attention on special laws*

According to section 10 of the Finnish Constitution, the data protection of personal data must be enacted in law. Due to this provision, there are currently up to 650 special laws legislating on the protection of personal data. With regard to the transfer of data between authorities, the general law to be applied alongside the Data Protection Act is the Act on the Openness of Government Activities. The tragic school shootings in Jokela and Kauhajoki highlighted the issue of the functioning of the whole legislative framework. Particular attention was paid to legislation on student welfare, firearms and health care. It was established that the authorities in various administrative sectors have not paid sufficient attention to the state of legislation. On the other hand, it was easy to observe that personnel who have to apply legislation at the local level have not received sufficient information and steering. Therefore, in problem situations, they were unable to act within even the permitted limits of legislation.

#### *Surveys conducted*

During the year under review, the Office of the Data Protection Ombudsman conducted several surveys. The national act on the electronic processing of client data within social welfare and health care entails a specific provision to appoint a person responsible for data protection in each unit. In addition, the act requires that the manager of each unit draws up specific, applicable data protection guidelines. According to the survey, the implementation of the provisions has started off well but the situation could still be improved. At the same time, wide-ranging education for persons responsible for data protection was launched, which at its most comprehensive is university level.

In the so-called web police survey, the Office of the Data Protection Ombudsman analysed the legality of processing personal data in Finnish web-based services. The survey focused, for example, on services providing social networking, services for children and young people and services collecting sensitive personal data. The results of the survey showed that a great deal remains to be done with regard to the fulfilment of the information obligation. Special measures were applied to some of the service providers surveyed.

The third survey assessed the functioning of the Personal Data Act and partly the criminal sanction system. In the survey the Office of the Data Protection Ombudsman analysed, among other things, the sentences passed by courts and decisions made by prosecutors. The survey showed that the number of data protection offences continues its slow but steady increase, which is thought to be caused by the improved communication on the rights for and significance of data protection, increasingly secure data systems, and the improved professional competence of the police and prosecutors. On the other hand, there was some discussion on whether the sanction system is strict enough.

#### *Scientific research*

Scientific research often deals with sensitive personal data. For research purposes, data is often needed from a variety of sources. Researchers seem to be often very insufficiently informed on the requirements set by data protection on scientific research. For this reason, the Office of the Data Protection Ombudsman implemented an extensive and comprehensive web-based guidelines project in cooperation with various authorities. The aim of the project was to improve the level of data protection in scientific research, to make researchers' work easier and to improve the practices of authorities functioning as sources of information. The project output includes

virtual guidelines together with their requisite quality assurance systems and several manuals determining best practices.

## **IRELAND**

We ratified the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows in May 2009. We also made a declaration regarding the application of the Convention to personal data which are not processed automatically but which are held in a relevant filing system. Furthermore, we updated our declaration in relation to the designated authority for the purposes of the Convention.

A Health Information Bill is being drafted. The Bill will establish a statutory framework to support the use of personal information throughout the health system to enhance patient care and safety and the achievement of wider health goals with proper regard for the privacy, confidentiality and security of such information.

The Minister for Justice, Equality and Law Reform established a Data Protection Review Group to examine the issue of data protection breaches

## **LATVIA**

### **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 repealed 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).



Identity Card (ID card) is the main document to prove identity and nationality, mandatory for every citizen of the Republic of Lithuania at the age of 16 who is not in possession of a Citizen's Passport issued prior to 1 January 2003. ID card can be issued to a person who is not 16 years old yet, if necessary. ID card is mandatory inside the country and can be used to travel abroad to countries with whom appropriate treaties and agreements have been concluded.

ID card as issued since 1 January 2009 complies with the requirements set in the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, and with recommendations of the International Civil Aviation Organization.

In accordance with the data included in the central database of the Population Register the following data related to the citizen are included in the ID card:

- name (names); surname; gender; date of birth; personal identification number; citizenship;
- it must contain citizen's face image and citizen's signature;
- since January the 1st, 2009 also by electronic means have been recorded the above

mentioned data as well as citizen's facial image and fingerprints, certificate for identification in electronic space and a qualified certificate.

The contact chip provides means for using the card online, because it complies with specifications of the European Citizen Card and contains both – a certificate for an online identification, and a qualified certificate for e-signature.

A contactless chip stores biometric data: face and fingerprints. The face image in the chip is the same as the one engraved and is stored in JPEG2000 format.

Personal identity card provides a possibility:

- to sign electronic documents by secure e-signature
- for information systems, other providers of services to identify a person, connecting to information systems and registers while sending data online.

### **1.3. Law on Electronic Communications**

On the 15<sup>th</sup> of March 2009 entered into the force Law No. X-1835 on Amendment of and Supplement to the Law on Electronic Communications of the Republic of Lithuania, the articles 1, 3, 7, 12, 34, 77, its section 9 and annex and Supplement with a new annex implementing the Data Retention Directive 2006/24/EC. According to this Law operators have an obligations to retain statistical electronic data 6 months.

#### *Secondary legislation*

#### *Resolutions of the Government*

1.4. On 1<sup>st</sup> January 2009 entered into the force Resolution No. 1182 of the Government of the Republic of Lithuania "Concerning the Resolution No. 1156 of the Government of the Republic of Lithuania of 25 September 2001 "On the amendment of structural reform of the State Data Protection Inspectorate, granting of authorization, the approval of State Data Protection Inspectorate Regulations and partial amendment of related Resolutions of the Government of the Republic of Lithuania" made according to the changes in the new wording of the Law on Legal Protection of Personal Data which entered into force from the 1<sup>st</sup> of January 2009.

1.5. On the 29<sup>th</sup> of April 2009 by Resolution of the Government of the Republic of Lithuania No. 366 „On Amending Resolution No. 807 of the Government of the Republic of Lithuania of 20 July 2005 Concerning the Approval of the Rules on Performing Inspections on Communications Confidentiality“ were adopted the Rules on Performing Inspections on Communications Confidentiality (Official Gazette, 2009, No. 53-2104).

#### *An orders of the Director of the State Data Protection Inspectorate*

1.6. On the 12<sup>th</sup> of November 2008 by Order of the Director of the State Data Protection Inspectorate No. 1T-71 (1.12) "On the Approval of General Requirements for the Organisational

and Technical Data Protection Measures” were approved General Requirements for Organisational and Technical Data Protection Measures. They specify the general requirements for organisational and technical data protection measures, which should be implemented by data controller and data processor to ensure personal data against any accidental or unlawful destruction, alteration, disclosure and against any other unlawful processing.

1.7. By Order No. 1T-4 (1.12) of the Director of the State Data Protection Inspectorate of 16 January 2009 “On Amending Order No. 1T-6 of the Director of the State Data Protection Inspectorate of 2 February 2006 „On the Approval of Rules for performing the prior checking” (Official gazette, No. 11-447, 2009) a new wording of Rules for performing the prior checking was set forth, establishing the procedure to be followed by data controllers in providing a notification to the SDPI on intended processing operations of personal data, regarding its content, order of provision and conduction of prior checking.

1.8. By Order No. 1T-5 (1.12) of the Director of the State Data Protection Inspectorate of 16 January 2009 “On the Approval of Description of Data Protection Measures Format” (Official gazette, No. 11-448, 2009) were adopted Description Format of data protection measures, to be submitted to the SDPI by data controllers in carrying out a prior checking and upon registration as data controllers also in the cases of processing of personal data by automatic means.

## **2. Case Law**

### *Handling of the Complain*

2.1. The Supreme Administrative Court adopted a decision in case on personal data announcement on Vilnius City Police Headquarters website.

The SDPI in January 2007 received complaints lodged by 2 persons regarding the personal data placed on the website of the Vilnius City Police Headquarters. After the investigation of complaints an instruction was issued to the Police to cease the publication of personal data of persons fined for road traffic offences (name, surname, date of birth, the time and locality of committed offence, the established extent of intoxication (drunkenness), article of Code of the Administrative Law Violations of the Republic of Lithuania, providing for the liability for the committed offence, sanctions applied for the said offence) on the Institution’s website for the purposes of informing the public, educational and prevention of administrative law offences.

Vilnius City Police Headquarters applied to the Vilnius Regional Administrative Court in respect of the issued Instruction and the latter by the decision of 26 June 2007 sustained a claim. However, after the judgment adopted by the Vilnius Regional Administrative Court was appealed against at the Supreme Administrative Court, the previous judgment was held true.

2.2. The SDPI on 8 February, 2008 issued instructions to some of the banks (hereinafter – banks) which are operating in Lithuania. The SDPI according to the request of the inhabitant of the Republic of Lithuania performed an inspection of lawful processing of personal data in six biggest banks. All these banks did not notify the claimant regarding the transfer of his personal data to the bailiff (the fact of money in cash and (or) money in cash in personal bank accounts) and did not specify the purposes for which the personal data were provided to the bailiff thereof breaching article 19(2) of the Law.

After the performed investigation according to the request there were issued the instructions to banks to ensure the compliance with provisions laid down in article 19 of the Law, i. e. to provide to data subjects in exercising their right of access to personal data a detailed and thorough information regarding the transfer of personal data to data receivers both by automatic and non-automatic means (in writing) by specifying the purposes of such transfer.

2.3. The SDPI carried out investigations of complaints received in January 2008 lodged by persons regarding the misdemeanour in office of the bailiffs and notary.

During the investigation it was revealed that the bailiff and notary without the legal grounds (not in discharge of their direct functions) were collecting personal data related to the real property owned by the right of private ownership from central data base in SE Centre of Registers, which administers the Register of Real Estate. Bailiffs and notary from the Real Estate Register have the right to obtain data solely for the discharge of their direct duties.

The instructions were issued to the bailiffs and notary to ensure that the reviews in the central data base of the Real Estate Registers should be performed only for the purposes of discharging of their direct functions.

2.4. Upon handling a personal complaint SDPI found out that one telecommunications Operator has obtained from the internet website of Communications Regulatory Authority of the Republic of Lithuania and is processing the subscribers' telephone communication numbers of other providers of electronic communications services. To these subscribers' of other electronic communications services providers the calls were made on behalf of Operator and offering to persons Operator's services – to introduce the electronic communications services provided by it and persuade the respondent into making use of such services.

The performance of direct marketing by using of electronic communications services is regulated by the Law on Electronic Communications of the Republic of Lithuania. It foresees, that the use of electronic communications services, including electronic mail, for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

According to the Law on Legal Protection of Personal Data of the Republic of Lithuania, the direct marketing is an activity intended for offering goods or services to individuals by post, telephone or any other direct means and/or inquiring their opinion about the offered goods or services. Furthermore, the Supreme Administrative Court of Lithuania in its ruling of 22 June 2006 (the administrative case No. N3- 733-06) stated, that "the subscriber's consent to use electronic communications services for the purposes of direct marketing, as foreseen by the Law on Electronic Communications, should be obtained prior but not at the (same) time of using direct marketing means". The Operator had no proof as regards subscriber's consent.

The SDPI issued the instruction to this provider of electronic communications services - to use electronic communications services for the purposes of direct marketing only after the prior consent is given by the subscriber, i.e., the consent must be obtained in advance, prior to using the electronic communications for the purposes of direct marketing, but not at the same time when using the electronic communications means.

#### *Inspections initiated by the SDPI*

#### 2.5. The Inspection of Commercial Companies Providing Quick Crediting Services

The SDPI, striving to find out the legitimacy and extent of processing of personal data of persons, applying to the financial institutions for quick credit services by internet or SMS, performed inspections on lawful processing of personal data at the six financial institutions.

The violations of the LLPPD were established in all financial institutions. One financial institution eliminated the violations during the inspection. The other financial institutions were issued instructions to eliminate the violations, also were provided instructions to other data controllers involved in processing of received personal data at the inspected financial institutions.

2.6. The Inspection of financial companies on legitimacy of personal data processing for the purpose of providing the investment services

The SDPI in order to find out the scope and legitimacy of data processing for the investment services purpose performed inspections on legitimacy of personal data processing in 27 financial companies, providing investment services (11 financial broker firms, 10 investment fund control companies, 6 credit companies).

The violations of the Law were established in 26 financial companies. Types of violations:

- Some of the financial firms are not included in the State Register of Personal Data Controllers and did not notify about the personal data processing for the purpose of providing investment services;

- processing data of amount different than notified to the SDPI;
- direct marketing regulation enforcement: the possibility for the data subject is not ensured to express his/her consent;

- data retention period had not been defined or defined improperly;

- adequate data protection measures were not implemented;

- adequate technical data security measures were not implemented.

The financial companies providing investment services were given instructions regarding these violations.

### **3. Other**

#### *Recommendations issued by SDPA*

##### **3.1. Secure Data Transfer by e-mail**

In November 2008 the SDPI drafted recommendation how to communicate data by email securely, i.e. how to send secure e-mails, which could be read only by the addressee and not by a stranger.

The letter sent by us goes through computer networks. If a correspondence is especially important, secret, confidential information or personal data, this is not secure (unless the proper safety measures are ensured). When sending a letter by e-mail, the threat arises concerning its content confidentiality and integrity. The electronic mail may be intercepted, read and, what is even worse, may be changed without your knowledge.

##### **3.2. Wireless Networks and Its Technologies, What is it?**

In December 2008 the SDPI drafted recommendation on data protection issues using wireless network and the risks which may arise.

Lithuania's Standard LST ISO/IEC:17799:2006 foresees, that in cases of accessing to the wireless networks, the additional personal identification control means should be applied. SDPA paid people attention that the wireless networks control means are to be especially carefully selected because the deployment of these opens far more possibilities for undetectable intrusion (hacking) to the data flow sent through the networks enabling information interception. Wireless networks should be separated from internal and private networks. Bearing in mind that it is not easy to define exactly the limits of wireless network the risk assessment should be carried out enabling to establish the appropriate networks separation management means (e.g. secure personal identification, encrypting techniques or selection of frequency).

#### *Publications*

##### **3.3. Attention! Excessive personal data**

„Justitia“ (2007 No. 4(66)) – a law science and case law magazine published an article of the Deputy Director of the SDPI Rita Vaitkevičienė under the title “Attention! Excessive personal data”.

The article presents an overview of tendencies related with the processing of personal data in the electronic media and looks into the issue of compliance with the principle of economy of personal data. It is attempted here to prove that the legal acts of the Republic of Lithuania fail to comprehensively determine to what extent personal data are to be processed in the electronic medium, but also to offer possible solutions of the issue. The article gives a short survey of the

aspects with which the courts are encountering in resolving the issues regarding the violations of the LLPPD due to the processing by data controllers the excessive personal data than it is necessary for the achievement of legitimate purposes.

#### 3.4. The Employee also Has a Right to Privacy

The magazine of Law science and practise "Justitia" (No. 2(68), 2008) published the article "The employee also has the right to privacy" drafted by the Deputy Director of the SDPI Rita Vaitkevičienė.

The article reviews what personal data the employer should and could require to provide, what personal data are he entitled to receive from other subjects and what level of privacy the employees may expect at the workplace, especially during the recruitment. The labour relations in a broader sense imply all the relations between the employers and the persons recruited, regarding the conclusion of working contract, carrying it out, the management of human resources, including the performance of commitments, envisaged in laws or specified by the contracts, also work management and etc.

The emphasis is placed on the fact that there are sufficient legal measures to ensure the privacy at the workplace, besides, labour relations generally by their nature are contractual, therefore the privacy level should also be agreed upon between the employers and the employees. The article brings forth an attempt to consider the peculiarities of the processing of personal data in all stages of the labour relations.

#### 3.5. Regulatory Developments in the Field of Personal Data Protection

The publication "Civil Service News" (January-February, 2009, No. 15, p. 36-39) have published an article "Regulatory Developments in the Field of Personal Data Protection" drafted by Head of Law Division of the SDPI Daiva Paulikienė.

According to the contributor, she took a favorable opportunity for discussing the main amendments and developments of the new wording of the LLPPD, adopted on 1 February of 2008 and enacted on 1 January of 2009.

### **MALTA**

- Transposition and coming into force of the Data Retention Directive 2006/24/EC in domestic legislation, in August 2008.
- Freedom of Information Act, which vests the Data Protection Commissioner with the additional function and duties of the Information Commissioner was enacted by the Parliament of Malta in December 2008. To date only some articles of this Act have come into force.
- In order to commemorate Data Protection Day 2009, the Office of the Data Protection Commissioner distributed in all schools, posters and mouse mats conveying a data protection message.

Mr Joseph Ebejer was appointed as the new Data Protection Commissioner, in February 2009.

## **SLOVAKIA**

### ***A. Legislative developments***

Minor, although by its meaning very important change in the area of legislative regulation governing the existence and functioning of the Office for Personal Data Protection of the Slovak Republic (hereafter referred to as „the Office“) has been performed. By adopting of the Act on the Prevention of Crimes and Other Antisocial Activities and on amending of other laws (Act No 583/2008 Coll) the budgetary status of the Office was adjusted. By this particular change the Act No 428/2002 Coll On Protection of Personal Data (hereafter referred to as "Act No 428/2002 Coll") was amended in regard to the "Personal Data Protection Budgetary Program" which was transferred from the budgetary category of the Government Office of the Slovak Republic to the General Treasury Administration category. By this transfer the independence of the Office in the budgetary field has been strengthened in the formal way. In the next budgetary year it shall not be necessary to submit the budget for the approval as a part of the Government Office's budget. The above mentioned solution, however, still leaves in the possibility or ignoring financial requirements of the Office because General Treasury Administration category is under the administration of the Ministry of Finance of the Slovak Republic whose budget is submitted to the negotiation and approval of the National Council of the Slovak Republic.

### ***B. Major case law***

In 2005 the Office issued the order addressed to the state administrative authority as a controller of the filing system whereby termination of the disclosure of national identification number (an identifier of general application) of data subjects on the website of the official journal was required. It was also imposed to the controller to remove already published national identification number on its website. Recipient of the order filed at the Office an objection against this decision which was rejected as unacceptable. The controller brought the question before the court requesting the cancellation of the Office's decision. The court dismissed the claim and in its opinion stated that making personal data public is very specific processing operation. Its particularity lies mainly therein that it is a process which can not be absolutely undone and brings about all range of consequences, which may have, in the case of unlawful disclosure, negative effect on data subject. Disclosing of national identification number is even more sensitive. Finally, the law explicitly prohibits the disclosure of identifier of general application. According to the court the decision of the Office was adequately reasoned and convincing and in accordance with the competence granted to the Office by law.

### ***C. Major specific issues***

#### **Inspection activity and disposing of notifications**

Inspection's Department of the Office performs the execution of independent supervision of personal data protection and is involved in the protection of fundamental rights and freedoms of natural persons by processing of their personal data. Activities of the Inspection's Department are mainly focused on the inspection of filing systems of controllers and processors and handling of notifications of data subjects and other individuals who claim to have been directly affected in their rights stipulated by Act No 428/2002 Coll.

#### **Supervision of personal data protection in figures**

In 2008 data subjects and other natural persons who claimed a breach of the protection of their personal data filed to the Office 113 notifications. Other 65 notifications were filed by other subjects who alleged the suspicion of violation of the Data Protection Act. The Chief Inspector of the Office ordered 74 proceedings against the controllers of filing systems to be conducted ex officio. Another 21 notifications were pending from the year 2007. Overall, the inspection department in 2008 dealt with 273 notifications. In this regard the Inspection's Department by the controllers and processors of filing systems conducted 105 inspections and 34 "submissions to



explanations". Altogether 75 orders were issued for removal of deficiencies determined by the inspection. The right to file an objection against the issued order had been used only by one controller. Objection was dismissed.

142 of 252 new notifications from 2008 were filed against the private sector controllers, 61 against controllers from public administration, respectively against the other public administration bodies. In 28 cases, the Office investigated notifications against self-government authorities. 8 cases related to the civil society organizations, foundations, political parties or movements and registered churches or religious groups. Public administration institutions were investigated in 4 cases. In 9 cases it was proved that the notification was filed against a subject who was not the controller of the filing system under the Act No 428/2002 Coll.

Of the 113 notifications filed by data subjects in 2008, the Office completed 99 cases, of which 71 were accomplished within the basic statutory period of 60 days. Longer investigation of other notifications was caused by the necessity of the consultations with other institutions, inspections of filing systems at a controller, by more exacting gathering of evidence or by the request for cooperation presented by the very petitioners. Total 50 of all handled notifications were evaluated as unfounded.

In case that informant is not satisfied with the disposing of his notification, he can submit to the Office repeatedly a notification within the statutory period of 30 days. From the 99 completed cases in 2008 only 2 repeated notifications were submitted to the Office. Remaining 97 informants whose notifications have been disposed of in 2008 respected the decision of the Office regarding the case, which is more than 96 %. During the year 2008 the Inspection's Department passed 4 notifications to the law enforcement agencies.

In 2008 Office imposed 14 fines in the total amount of 1 045 000 SKK (34 687, 65 €). Sanctions usually moved about the lower-bound of possible rates. The maximum penalty was imposed in the amount of 250 000 SKK (8298.5 €).

## **Nation-wide inspection activities of the Office**

### ***Inspections of video surveillance systems in towns and municipalities***

The Inspection's Department in 2008 carried on inspections of video surveillance systems. The nation-wide inspection was aimed at examining the video surveillance systems, whose operators are towns and municipalities. The Inspection's Department conducted in this respect 12 inspections, seven of which took place still in 2007. Deficiencies have been found out during all conducted inspections. In this regard the Office issued orders towards the controllers. The most common shortcomings lied therein that the controllers the monitored areas which are accessible to the public did not marked clearly as being monitored, they did not keep records of the filing system, failed to destroy the recordings within the period stipulated by Act No 428/2002 Coll and they failed to take due technical, organizational or personal measures in the form of security directive of camera filing system.

### ***Inspections aimed on processing of personal data by executors, notaries and attorneys***

The year 2007 has showed out that several executor offices went beyond the framework of the provisions of Act No 428/2002 Coll by disclosing the national identification numbers of the data subjects on the official notice board (announcement of the initiation of execution, auction notice). The inspections of executor offices accomplished in 2008 also revealed shortcomings in the application of provisions of the Act No 428/2002 Coll related to security of the processing of personal data, especially in those cases where the filing system processing the personal data is connected to Internet.

The Inspection's Office checked the status of compliance with the provisions of Act No 428/2002 Coll at selected notaries and law offices throughout the Slovak Republic. Examined was in particular:

- advising of entitled persons
- content of contracts between controllers and processors,
- keeping records of human resources and payroll filing system and client's information system
- authorization of a personal data protection official,
- existence and quality of security project, or security directives.

The orders were issued in connection with the elimination of shortcomings and after an in-depth analysis of the whole case discussed by the Chief Inspector with the competent representatives of the Slovak Bar Association, Slovak Chamber of Executors, Chamber of Notaries of the Slovak Republic who from their position can effectively provide the guidance to the competent subjects how to obtain a remedy as soon as possible.

### ***Inspections aimed on processing of personal data in the health sector***

In 2008 office dealt with several notifications of data subjects against the controllers in the health sector. Concerning to the number and importance of some of those notifications the Chief Inspector decided to realize inspections to check to what extent the controllers in health sector comply with the provisions of Act No 428/2002 Coll regarding the processing of patient's personal data. The Inspection's Department inspected state and private health care facilities (hospitals and surgeries), pharmacies and health insurance companies. Most commonly controllers failed to provide security directives which would clearly define the scope of competence and description of functions of entitled persons and the scope of their responsibilities in respect to what kind of operations those persons do with the personal data, even during some extraordinary situations (e.g. closure of a surgery, hospital or its move, etc.). Office in several numbers of cases identified indiscreet obtaining or disclosure of personal data in health care facilities and pharmacies. Also suspicions of leakage of personal data of newborns to the health insurance companies have been handled by the Office.

### ***Special inspection activities carried out in connection with the accession of the Slovak Republic to the Schengen area***

In connection with the preparation of the accession of the Slovak Republic to the Schengen area, the Inspection's Department pursued in 2008 further inspections in the selected embassies of the Slovak Republic abroad. Its aim was to examine compliance of the controllers of filing systems with the Act No 428/2002 Coll, procedures applied while issuing the Schengen visas and fulfilling of the requirements stated in the Schengen catalogue (recommendations and best practices) related to the visa's issuance. In March 2008 the consulate departments of the Slovak Republic embassies in Kuwait and Damascus were inspected and in May 2008 consulate departments in Prague and Brno. In regard to monitoring of legal processing of personal data in accordance to the present version of Schengen Information System (SIS I) the inspection was conducted in National Office of SIRENE, in the Office of International Police Cooperation and in the Presidium of the Police Force.

### ***International cooperation on complaints handling***

The Office regularly participates in spring and autumn international workshops for inspectors of the authorities for the personal data protection. At the autumn workshop in 2007, which was organized by the Portuguese authority for the protection of personal data in Lisbon, it was decided that the XVIII. International workshop for inspectors in autumn 2008 will take place in Slovakia. Workshop organized by the Office was held on 29 to 30 September 2008 in Bratislava. Except of the inspectors from the member states of the European Union, the workshop also attended inspectors from the candidate countries, which are preparing for joining the European Union. At the workshop took part overall 63 foreign participants and 10 office's employees. European Data Protection Supervisor's Office was represented by two delegates. The event was opened by the Chairman of Parliamentary Committee on Human Rights, Minorities and the Status of Women and the President of the Office. At the meeting, the inspectors dealt with five basic themes during the following panels:

1. Complaint Handling: Powers of supervisory authorities in the handling of complaints

2. Exchange of best practices from the inspections at the consular departments of the embassies regarding Schengen visa's issuance
3. Balancing of interests: Personal data protection vs. mass media
4. Application of security measures in the processing of personal data
5. Processing of employment personal data.

Inspection's Department presented the topics as follows:

- Execution of inspections and internal rules for inspection
- Giving of explanations and personal data protection official
- Entitled person; organizational and personal measures
- Legal framework and conditions for the preparation of a security project
- Legal framework for processing personal data by a video surveillance system and the experience of the Office in the exercise of inspections of video surveillance systems.

#### ***D. Trans-border personal data flow***

During the monitored period the Office issued 3 approvals of the trans-border flows of personal data. The subject of the trans-border data flow were personal data processed in the employment context, human resources management and outsourcing of processing operations. One decision on trans-border transfer to countries which do not ensure an adequate level of protection of personal data was issued for the controller – importer with its seat in India on the basis of compliance with legal provisions stipulating the need to incorporate the standard contractual clauses in the contract. Two decisions on transfer of personal data were issued by the Office for importers in the USA following the auto-certification of the importers in the Safe Harbor. On the basis of documents received it became evident that the controllers did not know how to properly use and interpret the relevant decisions of the European Commission, which were issued in connection to provide sufficient safeguards for the protection of personal data by and after their transfer to the third countries. The Office also dealt with requests for special registration of system for reporting suspicions of unlawful or unethical action (whistle blowing) and related requests for the approval of the transfer of such data to the processor in the USA. The Office also provided several opinions which interpret the Act No 428/2002 Coll and the opinions of Article 29 Working Party with respect to this issue. In the monitored period the Office issued one decision rejecting the special registration on the base of processing whistle blown data. After the removal of deficiencies, the Office allowed special registration in this case. In regards to whistle blowing no transfer of such data to third countries was permitted by the Office. After examining of the applications for approval of the transfer of personal data the Office came to conclusion that they did not contain the facts necessary for granting of an approval on the matter concerned. Those very wide whistle blowing systems went far beyond the scope of the Act No 428/2002 Coll. In this respect, it was solely about whistle blowing systems developed abroad, which were already set up and operating in the long term.

#### ***E. International cooperation***

Bilateral meetings are held for the purpose of addressing particular issues, arranging cooperation or for the exchange of best practices. Those meetings are attended by the president of the Office and competent experts.

- **May 2008** – Bilateral meeting with the Personal Data Protection of the Czech Republic initiated by the Slovak Office and taking place in Slovakia. Topics of the meeting were the issues which gave rise to the exchange of best practices on the performance of inspection activities:
  - Using of official documents in practice: identity card and passport in the light of European documents. Legislation concerning official documents, the scope of personal data in official documents
  - Processing and disclosing of personal data from central registers (filing systems) of the Ministry of Justice of the Slovak Republic regarding the jurisdiction (e.g. Official Journal of Court Decisions, Collection of Documents)

- Exercise of inspection at the controlled subjects (controller/processor) without giving the notice. Co-operation of the state administration authorities and other public administration bodies with the DPA in the Slovak and Czech Republic.

▪ **April 2008 – Visiting of the Office of General Inspector for Personal Data Protection in Warsaw, Poland.**

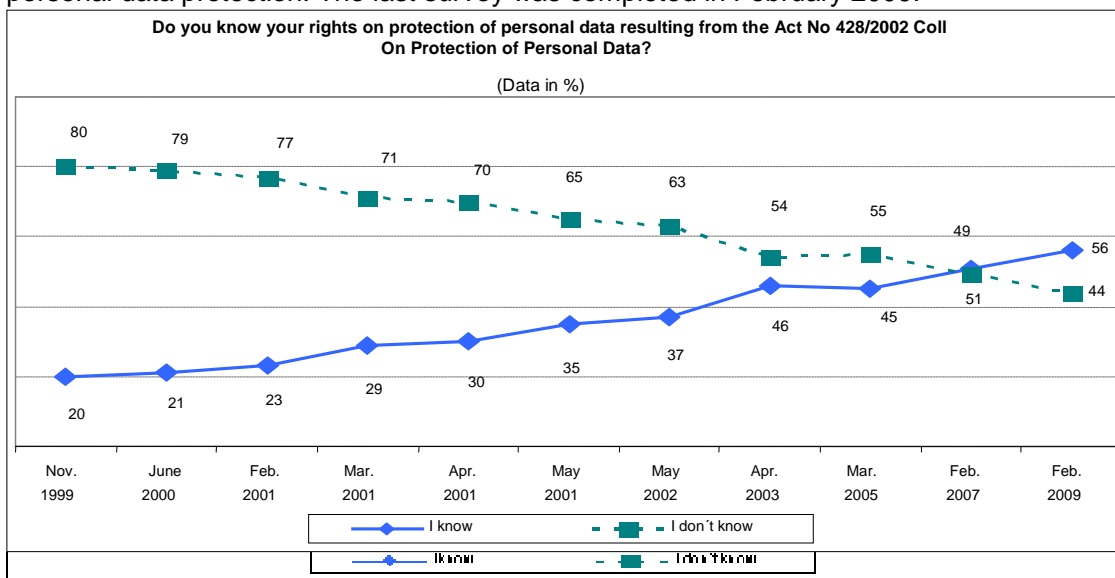
The purpose of the visit was to become familiar with the organizational structure and activities of the Polish DPA (GIODO). On this occasion presidents of the both DPA gave an interview to the daily newspaper „Rzeczpospolita“.

▪ **April 2008 – Visiting of the National Office for Personal Data Protection in Bucharest, Romania.**

The program of the visit was linked to the previous bilateral meeting in Bratislava with topic of the preparation of Romania’s accession to the Schengen area. Program was extended to the exchange of best practices, which were for instance related to the particularities regarding the independence of Romanian DPA.

**F. Public awareness on the protection of personal data**

The Opinion Research Institute of the Statistical Office of the Slovak Republic since 1999 conducted repeatedly on the order of DPA public opinion toll on some questions related to the personal data protection. The last survey was completed in February 2009.



As it can be seen from the graph, during the last two years - from February 2007 to February 2009 - the awareness of all categories of citizens about the rights on protection of personal data was increased by five percent. Altogether - from November 1999 to February 2009 – it has risen by 36 percent.

Generally it can be stated that the highest awareness (higher than the average for the whole Slovak Republic) have citizens of the age between 30 to 39 years (68%), 40 to 49 years (66%), respondents with university degree (87%), respondents with completed secondary education (67%) furthermore businessmen (70%), employees (74%) and citizens of the cities over one hundred thousand inhabitants (76%).

**G. Data Protection Day 2009**

To the commemoration of the annual Data Protection Day various activities aiming to address general public via mass media and Office’s web page have been performed.

The statutory television broadcasted on the 28th and the 30th of January 2009 two publicist sessions called FOKUS, wherein among the invited guests had been the president of the Office

and three other Office's employees. The topics of personal data protection has been zoomed in during the dialogs with moderators and by answering of questions posed by online spectators. On the Office's web page the „Question and Answer Forum“ has been realized, which consisted in addressing of questions of citizens posted during the respective TV broadcasting or by e-mails addressed ex post to the Office.

In the first edition of a new culture-and-society magazine the interview with the president of the Office has been published. From this interview the readers could obtain information relating the Office, their rights as the citizens in coincidence with the data protection legislation, pertinent risks and about the steps which could be taken in relation with their own personal data protection execution.

The new 'Ten Commandments of Data Protection' were elaborated which serve as a brief prevention manual for citizens in their daily life, e.g. by the handling of their personal documents, by their use of internet and in communication in general.

## **THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA**

### **REPORTING PERIOD**

1<sup>st</sup> September 2008 – 31<sup>st</sup> August 2009

### **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 28<sup>th</sup> 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
<b>Total:</b>	<b>75</b>

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 following inspections have been performed:

Type of inspection	Performed supervisions
<b>Regular</b>	<b>37</b>
<b>Irregular</b>	<b>37</b>
<b>Control</b>	<b>1</b>
<b>Total:</b>	<b>75</b>

Also, with the Annual program for performing inspection of the Directorate for the third quartile are projected/planned 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

<b>Chambers of commerce</b>	<b>4</b>
<b>Education</b>	<b>11</b>
<b>Legal persons</b>	<b>15</b>
<b>Associations</b>	<b>1</b>
<b>Security</b>	<b>1</b>
<b>Judiciary</b>	<b>1</b>
<b>NGO</b>	<b>1</b>
<b>Social security</b>	<b>1</b>
<b>Post</b>	<b>3</b>
<b>Total</b>	<b>503</b>

***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
<b>Total</b>	<b>30</b>

- ***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 REQUESETS
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	/	/
<b>TOTAL:</b>	<b>82</b>	<b>36</b>	<b>32</b>	<b>14</b>	<b>5</b>

- **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
<b>Total</b>	<b>187</b>

- **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 28<sup>th</sup> 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 ILECU's 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 ILECU's 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 ILECU's, 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.

## UNITED KINGDOM

### Major developments in the data protection field since the 24<sup>th</sup> meeting of the T-PD

- In November 2007, the Prime Minister commissioned the Cabinet Secretary's Data Handling Report in response to the child benefit data loss. The final report on *data handling procedures across government* was published on 25 June 2008. It set out how Government is improving its arrangements around information and data security, by putting in place core protective measures, getting the working culture right, improving accountability and scrutiny of performance. All departments are now required to carry out privacy impact assessments to assess the impact of new policies and practices on the use of personal data, ensuring that proposals are necessary and proportionate and comply with the Data Protection Act 1998 (DPA). Further scrutiny is provided by the Information Commissioner who can and does raise questions on planned policies or measures involving the processing of people's personal information.
- In October 2007 – before the data loss incident came to light – the Prime Minister invited Richard Thomas, the UK Information Commissioner, and Dr Mark Walport, to undertake an independent review of the framework for the use of personal data in both the private and public sector. Objectives of the review were to establish whether there should be any changes to the way the DPA operates in the UK and to explore options for implementing any possible changes. The review was published on 11 July 2008. Informed by the Review's recommendations, the Ministry of Justice launched a consultation on the Information Commissioner's inspection powers and his data protection funding.
- We are legislating in the Coroners and Justice Bill, currently before Parliament to make available to the Information Commissioner's Office the power to assess, without consent, central Government Departments and Public Authorities' compliance with the DPA; the power to impose a deadline and location for providing information relating to investigations; and the power to require any person, where a warrant is being served, to provide any information required to determine compliance with the DPA. These additional powers will ensure the regulatory framework is robust, proportionate and encourage good practice.
- The Criminal Justice and Immigration Act 2008, which received Royal Assent on 8 May 2008, amended the DPA and introduced a power for the Information Commissioner to impose a Civil Monetary Penalty for a serious, deliberate or reckless breach of the data protection principles of a kind likely to cause substantial harm or substantial distress. We are working to develop the necessary secondary legislation and guidance to support the commencement of these powers and to finalise the details of how this new power will operate.
- Christopher Graham was appointed as the next Information Commissioner with effect from 29th June 2009 for a period of 5 years.



## APPENDIX IX – INFORMATION ON THE 2009 DATA PROTECTION DAY

**Information given by member States on activities carried out on the occasion of the Data Protection Day<sup>3</sup>**

Please consult [Document DPC \(2009\) COMPILATION](#) on our Website.

---

<sup>3</sup> Further information available on : [http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/data\\_protection/Data\\_Protection\\_Day\\_default.asp#TopOfPage](http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Data_Protection_Day_default.asp#TopOfPage)