



Strasbourg, 22 June 2012

T-PD (2012)02Mos_Rev

**CONSULTATIVE COMMITTEE OF THE CONVENTION
FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING
OF PERSONAL DATA
(T-PD)**

**LE COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES
PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ
DES DONNÉES A CARACTÈRE PERSONNEL
(T-PD)**

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

Information sur les développements récents intervenus dans le domaine de la protection des
données au niveau national

TABLE OF CONTENTS / TABLE DES MATIERES

ALBANIA / ALBANIE.....	4
ANDORRA / ANDORRE.....	12
AUSTRIA / AUTRICHE.....	13
BOSNIA AND HERZEGOVINA / BOSNIE-HERZÉGOVINE.....	15
CROATIA / CROATIE.....	18
CYPRUS / CHYPRE.....	23
CZECH REPUBLIC / REPUBLIQUE TCHEQUE.....	24
ESTONIA / ESTONIE.....	25
FINLAND / FINLANDE.....	26
GERMANY / ALLEMAGNE.....	27
ICELAND / ISLANDE.....	31
IRELAND / IRLANDE.....	32
ITALY / ITALIE.....	33
LATVIA / LETTONIE.....	35
LIECHTENSTEIN.....	36
LITHUANIA / LITUANIE.....	37
LUXEMBOURG.....	38
MALTA / MALTE.....	42
MONACO.....	43
MONTENEGRO.....	44
NORWAY / NORVÈGE.....	48
POLAND / POLOGNE.....	49
PORTUGAL.....	52
SERBIA / SERBIE.....	53

SLOVENIA / SLOVÉNIE.....	55
SWITZERLAND / SUISSE.....	62
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA /	
L'EX-REPUBLIQUE YOUGOSLAVE DE	
MACEDOINE.....	64
UKRAINE.....	68
UNITED KINGDOM / ROYAUME-UNI.....	69

ALBANIA / ALBANIE

Issuing and approving administrative acts, the giving of opinions and institutional cooperation.

Authority of the Commissioner pursuant to the enforcement "Law on the Protection of Personal Data":

- **There drafted and was approved in date 26 April 2012 in the Albanian Parliament amendments to the Law Nr. 9887, dated 10.03.2008 "On personal data protection".**

One of the main activities of the DPA was to review the Data Protection Law and work on its harmonization with the EU standards and more specifically the Directive 95/46/EC. The amendments have intended to enrich with new definition, but also amending existing ones. Also we have expanded the areas in the rights of the data subject. The data subject carries the right to ask for the blocking of them, in any case he deems that they are "irregular, untrue, and incomplete", or have been processed and collected against the law. Also have been increased sanctions against controllers that violate the principles of protection of personal data, etc.

- **There is drafted and approved Instruction No. 12, dated 21.12.2011 "On the Control of Identity at the entrance of buildings";**

This instruction regulates the certain rights and obligations of building owners or managers, who are in the position of controller at the entrance of a building or area, should meet the obligations defined in the law for protection of personal data. Instruction will help in prevention of cases of violations of the rules on processing personal data, as well as guaranteeing the rights and freedoms of individuals, and in particular the right to privacy.

- **There is drafted and approved Instruction No. 13, dated 22.12.2011 "On some additions and changes in Instruction no. 3, dated 05.03.2010 "On CCTV surveillance system in buildings and other premises"";**

The aim of this instruction is to improve existing provisions of the act support based on practices that are encountered during the inspections conducted in different controller from the relevant Department on DPA.

- **There is drafted and approved Instruction No. 14, dated 22.12.2011 for "processing, protection and security of personal data in electronic communications sector of the public";**

This instruction has a goal of producing an equivalent level of protection of human rights and fundamental freedoms and in particular the right for privacy, taking into account the processing of personal data in electronic communications sector and to ensure free movement of the data and of the equipment in electronic communications services in the country.

- **There is drafted and approved Instruction No.15, dated 23.12.2011 "On processing and publication of personal data in the judicial system";**

This Instruction was prepared by the Commissioner for Personal Data Protection with the support of the experts of the project EU-IPA 2009 "Strengthening the Office of the Commissioner for Personal Data Protection".

It aims to establish the rules regarding the processing, publication of personal data and the security measures, in the framework of the protection of personal data, in a particular sector such as the judicial system. Also addresses the obligations of the responsible persons during the publication of court decisions, civil, penal, commercial, family and the case when the parties are minors.

- **There is drafted and approved Instruction No. 16, dated 26.12.2011 on "Protection of personal data in the direct marketing and security measures";**

This instruction has intended to protect personal data and taking measures of security during their processing. There are sanctioned the provision relating to informing the data subject about the processing their data's, obtaining consent and revoke of it at any time, etc.

- **There is drafted and approved Instruction No. 17 "On determining the time of retention of personal data processed in electronic systems, by the state police for the purposes of prevention, investigation, detection and prosecution of criminal acts".**

This Instruction has been prepared with the support of the experts of the project EU-IPA 2009 "Strengthening the Office of the Commissioner for Personal Data Protection" in the framework of assistance for drafting of legal and sublegal acts in accordance with the law on personal data protection and in collaboration with the General Directorate of State Police.

It aims to establish rules on the time of retention of personal data in electronic systems and more specifically the management procedures of the data in order to respect the review deadlines of the time of retention by the state police officer, in the framework of the protection of personal data.

- **There is drafted and approved Manual on Evaluation of Requests for Approvals of Data Transfers to Foreign States.**

The manual was prepared with the support of EU experts IPA 2009 project " Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards " in the framework of assistance for drafting sublegal act and regulations in accordance with the law for protection of personal data. Aims at defining the rules for sending personal data in other countries respect the rules provided in law. In the manual determined the level of protection of personal data for a state to evaluate all the circumstances relating the processing, the nature, scope and duration, country of origin and final destination, legal and safety standards in force in the recipient state.

- **There is drafted and approved in cooperation with IPA Project, Manual on "" Some changes and additions to the manual "Administrative Investigation of the Commissioner for Personal Data Protection", "approved by Order 83, dated 15.09.2010 of the Commissioner;**

Amendments in this manual consist in the determining in more clearly the detailed rules for the development of administrative investigation, starting from the meaning of administrative investigation, the investigation form, stages of investigation, the beginning of the investigation, final report up to the review of the report and the relation by the Commissioner and taking final decisions on his part.

- **There is drafted and approved the Manual "On the procedures of notification."**

The manual was prepared with the support of EU experts IPA 2009 project "Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards ". This document provides information and guidance to the Department staff regarding the

steps that should be taken in the notification procedure for its to successfully termination. The manual also contains additional information about some issues and / or problems relating to notification procedure.

- **There is drafted and approved the Regulation on "Protection of personal data and their security," Commissioner for Personal Data Protection;**

This act has to define the rules and principles for the protection and lawful processing of personal data and security measures to protect personal data which are administered by the Commissioner for Personal Data Protection.

- **There is drafted and approved the Institutional Strategy of the Commissioner for Personal Data Protection for the period 2012-2013 and Action Plan;**

Strategy 2012-2013 for the protection of personal data was drafted thanks to the efforts and dedication that should be indicated for safety of citizens and protection of their personal data. The vision of this strategy is that Albania is a safe environment, to enforce the law and where protection of personal data being under control.

- **There is drafted and approved the Strategy for the trainings in the Commissioner for Personal Data Protection.**

The act was prepared with the support of EU experts IPA 2009 project " Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards " the aims is to improve the effectiveness and performance of human resource management staff of the Commissioner.

- **It has given a legal opinion on the Penal Code of the Republic of Albania.**

Drafting of proposals for some amendments to the Criminal Code was based on international laws, specifically referring in the proposals given by the Czech and the Polish standard. Opinion consists in the inclusion of provisions on unlawful processing of personal data and relevant measures of punishment.

- **It has given a legal opinion on the Civil Code of the Republic of Albania.**

For their preparation we are assisted by the experts of the project EU-IPA 2009 and the amendments refer mainly to the Czech standard. The amendments consist in the inclusion of certain provisions concerning the protection of human dignity. Specifically it provides the principles of the protection of human dignity and the rights before and after death.

- **Amendments have been prepared to the Law No. 8951, dated 10.10.2002 "On the Identification Number of Citizens".**

With the support of EU experts IPA 2009 "Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards" are preparing the amendments of the Law No. 8951, dated 10.10.2002 "On the Identification Number of Citizens". The object of supplements to the Law no. 8951, dated 10.10.2002 was the implementation of legal provisions for the protection of personal data after each operation performed by the number of identity in law enforcement for the protection of personal data is processed.

- **Amendments have been prepared to the Law No. 9662, dated 18.12.2006 "On Banks in the Republic of Albania", Law No. 9917, dated 19.05.2008 "On Prevention of Money**

Laundering and Financing of Terrorism“ and Regulation No. 67, dated 13.10.2010 "On the information content and functioning of Credit Registry at the Bank of Albania”;

- **It has given a legal opinion on the Draft Law "On Foreigners“**

In this framework we have suggested the unification of the terminology of this draft law with the terminology used in the law on personal data protection. Also are proposed corrections in some of the articles concerning the management of personal data and the inclusion of an article relating to the security and confidentiality of personal data.

- **It has given a legal opinion on the Draft Law “On weapons”;**

- **Have been prepared amendments in Law no. 9747, dated 4 June 2007 "On State Police" and Law. 8792, dated 10 May 2001 "On the establishment of the Center of Data Processing“**

These amendments have been prepared with the support and assistance of the experts from the project EU-IPA 2009 "Strengthening the Office of the Commissioner for Personal Data Protection".

In the content of the law "On State Police" is proposed the involvement of a new chapter entitled "The Processing of Personal Data", which provides specific provisions on obligations of the police authorities during the processing of personal data.

In the content of the law "On the establishment of the Center of Data Processing" is proposed the change and the involvement of some terms in order to harmonize it with the law on data protection. Also are requested clarifications of some articles.

- **It was given a legal opinion on the draft decision "On approval in principle of the Optional Protocol to the Convention on the Rights of the Child “On communication procedure””.**
- **It has given a legal opinion on the “Draft Agreement between the Council of Ministers of the Republic of Albania and the Government of Georgia on cooperation in the fight against crime“.**

The agreement aims to develop bilateral contacts, providing assistance and cooperation in the fight against terrorism, organized and international crime. Also with this agreement is intended the exchange of information and experience. In this agreement is provided the protection and the exchange of personal data among the Parties.

- **It has given a legal opinion on the draft agreement on “Social Protection”, between the Government of Albania and the Government of Hungary.**

In this draft agreement the Commissioner has given legal opinion on Article 37, "Data protection". The opinion consists in taking the necessary measures to ensure the appropriate level of protection of data taken during interception as well as to maintain confidentiality in accordance with the law "On protection of personal data".

- **On November 2011 was signed the cooperation agreement between the Commissioner for Personal Data Protection and the Steering Committee for the Protection of Personal Data of the Republic of Macedonia.**

This cooperation agreement was implemented to regulate the exchange of experiences, best practices and knowledge between experts of the two legislative institutions on the development, exchange of experience in the field of new technological developments, the transfer of personal data, etc.

- **On May 2012 was signed the cooperation agreement between the Commissioner for Personal Data Protection and the General Prosecutor's Office**

The agreement strengthens the scope of cooperation between the two institutions during the process of drafting and implementing regulations that guarantee the security of personal data and the processing that takes place during prosecution.

- **It is prepared the Leaflet "Beware of identity theft."**

This leaflet provides several cases in which individuals are vulnerable to data theft, and gives some advices on how to protect ourselves from the "thieves" of identity.

- **It is prepared the Leaflet "Protection of personal data for social services"**

- **Complaint Handling and Inspections**

- ✓ Over 50 Complaints handling;
- ✓ Accuracy and information on the data processed through the TIMS system - state police;
- ✓ Regarding the publication of personal data in the official website of the National Registration Center;
- ✓ Regarding the publication of personal data to a information website, without the consent of the data subject;
- ✓ Regarding the deregistration of a business (physical person) by the National Registration Center;
- ✓ Regarding the information provided by police authorities to a court of justice;
- ✓ Regarding a promotional phone call by a controller that implements such services to a mobile phone number.

- ✓ 43 Administrative Audit and Inspections-Recommendations, for this topics:
- ✓ Drafting of internal regulations on the security of personal data processed and confidentiality;
- ✓ Non compliance with the duty to notify;
- ✓ Non compliance with the duty to inform the data subjects;
- ✓ Processing of data without the consent of the data subject;
- ✓ Excessive data processing and not in proportionality to the purpose;
- ✓ Failure to have into place and to apply criteria for data security;

- ✓ Excessive Disclosure of some specific data on the purpose to inform the public and data subject, and not making the data anonymous;
- ✓ International transfer and disclosure of the personal data in violation to the Law on data protection and to the administrative acts of the Commissioner.
- ✓ 35 Fines to Data Controllers.

➤ **Complaint Handling and Inspections**

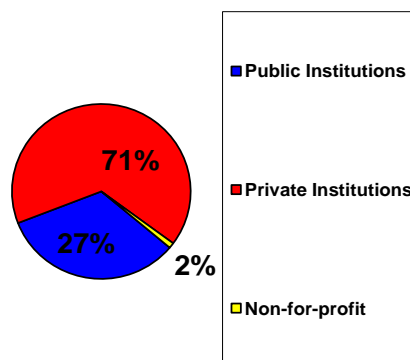
The Recommendations aimed at:

- ✓ Drafting of internal regulations on data protection and security of data;
 - ✓ Placing public notices in relation to monitoring-recording cameras (CCTV);
 - ✓ Technical security of data;
 - ✓ Fulfillment of the obligation to notify to the Commissioner's Office;
 - ✓ Obtaining consent and fair legal treatment of data subject;
 - ✓ The time retention of personal data.
- ☐ Blocking and deletion of data.
 - ☐ Fines for not notifying to the Office.

○ **Notification and Registration**

The process of notification-Statistical Table

- ☐ Banking sector;
- ☐ Healthcare;
- ☐ Insurances;
- ☐ Telecommunications;
- ☐ Education;
- ☐ Public sector.



Notifications	
Public Data Controllers	712
Private Data Controllers	1803
Total	2515
Registered	2205

➤ Foreign Technical Assistance

✓ EU-IPA Project 2009

- ☐ Implemented the most part of the activities foreseen in the working plan of the project compiled by the consultant FIIAP-Progeco in accordance with needs and in cooperation of the Beneficiary (KM DP) and approved by the EU Delegation (Contracting Authority);
- ☐ Commissioner requested officially EUD for extension to continue the project activities-Approved.

✓ Partnership Agreement, "Traveling with Privacy", Macedonia-Albania

- ☐ Application
- ☐ Under EU Programme "IPA CBC Call for Proposal"
- ☐ Technical Evaluation
- ☐ Reply, possibly September-October

➤ **European and International Activities**

- ✓ On 2 and 3 November 2011, the Commissioner took part in the 33rd International Conference of Commissioners of the Data Protection and Privacy in Mexico, "Privacy: Global Age." In the Conference were present Commissioners and representatives of controllers from different countries.
- ✓ On 13-18 November 2011, was made a training study visit to the Spanish Authority of Data Protection and Authority of Data Protection in Madrid, Spain. In this visit, most important was the introduction to the activity and experience of those authorities in the field of data protection and experience gained.
- ✓ On 24 and 25 November 2011, the Commissioner participates in the Regional Conference, "Strategic Approach for the development of mechanisms for the protection of personal data ", held in Skopje, Macedonia. The event was organized by the Macedonian authority for the Protection of Personal Data. In this event, was held a presentation on behalf of the Albanian authority of Data Protection on "Strategies

and implementation of the law on personal data protection in the Republic of Albania. In this framework, was also signed a cooperation agreement between the Albanian Commissioner of Personal Data Protection and the Directorate of Personal Data Protection of Macedonia.

- ✓ Commissioner for Data Protection in cooperation with IPA project "Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards" on 13 December 2011 organized the workshop "Processing of personal data in the sector of law enforcement". Participants were from State Police, Ministry of Justice and General Prosecutor's Office.
- ✓ On 27 January, with the assistance of IPA project "*Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards*", in the premises of the Information Center of the EU in Tirana, was organized an awareness-raising activity in the occasion of 28 January, the European Day of Data Protection. This event was attended by representatives of the Commissioner for Data Protection and the IPA Project, who shared with data subjects key messages on privacy and personal data protection. Also, different awareness materials were distributed. The purpose of organizing this event was the creation of an environment to discuss about the protection of personal data and therefore to achieve a higher level of awareness for the citizens (as subjects of personal data protection law). The presence of the media in this event was significant.
- ✓ Commissioner for Data Protection in cooperation with IPA project "Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards" on 26 January 2012 organized the workshop "Processing of personal data on banks sector".
- ✓ Commissioner for Data Protection in cooperation with IPA project "Strengthening of the Office of the Commissioner for Data Protection in Albania for aligning with EU standards" on 11 April 2012 organized the workshop "Processing of personal data on telecommunications sector".

ANDORRA / ANDORRE

La Journée de la protection des données en Andorre s'est centrée cette année sur le traitement de données à caractère personnel par l'administration. L'Agence a publié un guide qui a fait l'objet d'une large diffusion i qui détaille les actions qui peuvent être entreprises et les précautions qui doivent les entourer.

En ce qui concerne la législation, il est à noter qu'aucune modification de la Loi sur la protection de données à caractère personnel n'a été présentée au cours de cette période, donc ce qui est rapporté ici c'est la législation que dans des domaines spécifiques ou à des fins spécifiques développe des règles de protection de données personnelles :

« Règlement sur le Registre d'occupation hôtelière » (Contrôle des voyageurs dans les hôtels et maisons d'hébergement)

« Règlement sur la publicité pour les médicaments destinée au public

« Décision du Conseil du 18 janvier 2011 relative à la signature, au nom de l'Union européenne, et à l'application provisoire du protocole étendant aux mesures douanières de sécurité l'accord sous forme d'échange de lettres entre la Communauté économique européenne et la Principauté d'Andorre (publiée au Bulletin officiel le 30 novembre 2011)

Au sujet de la demande de Google pour la mise en œuvre de son service Street View en Andorre, l'Autorité de contrôle a en outre adoptée une recommandation visant à respecter de manière appropriée les principes de la protection des données. Google a approuvé nos exigences sur tous les points essentiels (la recommandation se trouve accessible sur le site internet www.apda.ad)

AUSTRIA / AUTRICHE

Major developments in the data protection field in Austria since December 2011

The following major developments have taken place/occurred:

- 1) *Agreement between the Government of the Republic of Austria and the Government of the United States of America on enhancing cooperation in preventing and combating serious crime (PCSC Agreement)*

The PCSC Agreement – which is modelled after the Prüm Agreement – provides for the mutual automated querying of dactyloscopic data and of DNA profiles for preventing and combating serious crime. The agreement also contains provisions on data protection and data security. Individuals can exercise their rights to access, correction, blocking or deleting of data via their national data protection authorities.

The text of the PCSC Agreement is available on the website of the Austrian Parliament (http://www.parlament.gv.at/PAKT/VHG/XXIV/VI_01388/imfname_229301.pdf).

The Austrian Data Protection Council, the advisory body of the Federal Government and the Governments of the Länder, dealt with the PCSC Agreement again in its meeting on 20 January 2012. The position adopted by the Data Protection Council is available in German at <http://www.bka.gv.at/DocView.axd?CobId=46383>.

The Austrian Parliament voted in favour of the PSCS Agreement.

According to Art. 27 para 1 of the PSCS Agreement it will enter into force – with the exception of Art. 7 through 9 (automated querying of DNA profiles) – on the date of the later note completing an exchange of diplomatic notes between the Parties indicating that each Party has taken any steps necessary to bring the Agreement into force. Art. 7 through 9 will enter into force following the conclusion of the implementing agreement(s) referenced in Art. 9 and on the date of the later note completing an exchange of diplomatic notes between the Parties indicating that each Party is able to implement those articles on a reciprocal basis. The exchange shall occur if the laws of both Parties permit the type of DNA screening contemplated by Art. 7 through 9.

2) Data Retention

The Austrian Acts (Telecommunication Act, Security Police Act and Criminal Procedure Act) transposing the EU Data Retention Directive entered into force on 1 April 2012.

3) Notification/Prior Checking

The Federal Chancellor has proposed a new regulation to facilitate notifications to the Data Protection Authority and prior checking according to Art. 18 and Art. 20 of Directive 95/46/EC. The idea is to notify the Data Protection Authority only with online-forms. The content of these forms is screened by a computer programme. If this programme does not detect any intended data processing which would require prior checking, the notification is accepted automatically. As a result, the time necessary for notifications would be reduced significantly, the Data Protection Authority would be relieved and the waiting time for controllers reduced. The envisaged entry into force of the regulation is September 2012.

4) Transparency Data Bank

The Transparency Data Bank should enable each individual to check whether he/she receives any subsidy from a public body or a body controlled by a public body and to get an overview over all possible subsidies and their prerequisites. In turn, authorities responsible for granting subsidies should have access to the data bank to check whether an applicant (still) satisfies the criteria for receiving a subsidy. Legislative proposals have been presented by the Ministry of Finance. From a data protection point of view it will be of extreme importance to make sure that authorities will get access only to those data in the data bank that they need for checking the prerequisites for a certain subsidy, thus not being able to see all subsidies already granted by other authorities. The project is still ongoing and has been on the agenda of the Data Protection Council.

5) Security Police Act

An amendment of the Security Police Act (Sicherheitspolizeigesetz) entered into force on 1 April 2012. It allows the police inter alia to observe individuals (before the police could only observe groups) suspected of committing – future – terrorist acts and to use personal data for the defence against threats directed against certain public institutions.

BOSNIA AND HERZEGOVINA / BOSNIE HERZÉGOVINE

Personal Data Protection Agency in Bosnia and Herzegovina was established by the Law on Personal Data Protection (Official Gazette of Bosnia and Herzegovina, No. 49/06) and commenced its operations in June 2006. In 2011 year the Parliamentary Assembly has adopted the Law on amendments to the Law on personal data protection (Official Gazette of Bosnia and Herzegovina No. 76/11)

45 working places were systematized by the Regulation on Internal Organization. Currently the DPA employs 24 staff members, of which 6 are new civil servants employed in early 2011 and 2 civil servants in 2012.

Supervision

In the reporting period Personal Data Protection Agency (hereinafter: the Agency) in accordance with its responsibilities has performed supervisions, proceedings ex officio, acted on complaints of citizens and gave expert opinions regarding processing and protection of personal data.

Most of the inspections referred to public bodies and the bodies of administration, the area of health and the private sector (ministries, clinical center, banks, shopping centers, the High Judicial and Prosecutorial Council). The subject of inspections was the lawfulness of processing personal data in the records of fingerprints (AFIS), the legality of collecting photocopies of identity cards and other personal documents when purchasing vouchers for transportation, control of the legality of processing personal data when closing a bank account, and deficiencies relating to the failure obligations prescribed by the Law and other laws that are required to apply to the processing of personal data. A total of 9 inspections have been performed in the reporting period.

Decisions issued ex officio have been related to illegal submission of data from criminal records during the security checks, unauthorized disclosure of personal data, illegal personal data processing and disclosure of personal data on the official websites.

The largest number of data subject complaints has been related to illegal request for submitting the medical certificate and certificate on criminal records during employment procedure, legality of disclosure personal data on the official websites and retaining the certificates by the employer, processing of personal data on health condition, use of personal data in purposes for which they are not intended and illegal request for insight in identity card and processing of personal identification number when paying bills.

A total of 34 decisions have been issued in the reporting period on data subject complaints, complaint of controller and ex officio.

A large number of subjects have also been processed in the reporting period on the requests for giving opinions of public bodies, as well as legal and natural persons.

The largest number of opinions has been issued regarding the following issues of personal data processing: disclosure and availability of the charges on the websites of research reporting, personal data processing for journalistic purposes and disclosure of personal data in the newspaper article, public video surveillance and public records presentation, transmission of personal data abroad, obligation of submission documentation to the contest procedure, establishing of the personal data collection, wages and incomes of employees and access to such information, legal basis for personal data processing, legality of establishing of the special Registry Book, marketing agencies obligation of notifying customers before further contacting for marketing purposes, security measures when using mobile communication, establishing

database of citizens, personal data processing and making it available to the third persons without consent of data subject, making personal data available to the third persons in the fee purpose, disclosure of personal data on the notice boards in residential buildings, coping of identity card, personal data processing of personal identification number by the banks, personal data processing through Internet portals and forums, using of personal identification number by police and providing data to the third persons, collecting data on ancestors and the kinship ties related to them, medical implants (pace makers), employer's rights to require from employees nationality declaration.

The Agency has issued a total of 72 opinions in the reporting period.

According to the Law the Agency maintains a Central Registry representing electronic record of basic information on data collections kept by controllers and it is aimed to inform data subject which personal data can be processed by controller and for which purpose. A total of 630 data collections have been entered into Central Registry in the reporting period.

During the reporting period a misdemeanor warrant has been issued to the Minister of Justice of Federation of Bosnia and Herzegovina as the responsible person for requiring submission of certificate on criminal records with the application procedure for public invitation for the appointment of experts in Federation of Bosnia and Herzegovina published by Ministry of Justice. According to the Law on Criminal Procedure of Federation of Bosnia and Herzegovina nobody has right to require from citizen to submit evidences on his/her conviction and it follows that Minister of Justice of Federation of Bosnia and Herzegovina responsible for illegal processing of personal data from criminal records that fall within the special category of personal data. The misdemeanor warrant has not been realized because the accused person requested for court decision.

Maglaj municipality has initiated administrative dispute against Agency's decision adopting complaint of the data subject because there was no valid legal basis for submission of the marriage certificate to the interested person in order to initiate enforcement proceeding. The Court of Bosnia and Herzegovina has made decision annulling the decision of the Agency. The Agency has filed a request for a reviewing of the Court decision considering that issuing of certificates from Register Books without determining of the legal interest is unacceptable and that it means violating privacy of the data subject, and finally the Court of Bosnia and Herzegovina made decision in the favor of the Agency.

After the inspection in the Central Election Commission of Bosnia and Herzegovina the Agency has instructed the termination of the personal data processing by publishing scanned statements on the property status of the candidates and elected persons on the official website. The Council for the Administrative Disputes of the Court of Bosnia and Herzegovina has acknowledged the complaint of the Central Election Commission of Bosnia and Herzegovina by its judgment and annulled the decision of the Agency. Dissatisfied with the decision of the Court, the Agency has filed a request for a reviewing of the Court judgment. The Appellate Administrative Council of the Court of Bosnia and Herzegovina has acknowledged the request of the Agency and amended the judgment of the Council for the Administrative Disputes so the lawsuit is dismissed.

A total of 2 administrative disputes have been closed and another one is in the proceeding.

In accordance with very limited financial resources, the Agency participates in international conferences and different trainings related to personal data protection.

Within the TAIEX project for assistance to the Agency, the training of the civil servants on personal data protection in medical sector was organized on 23 and 24 April, 2012. The aim of this training was to pay more attention to the personal data protection in medical sector in

Bosnia and Herzegovina. The education on the protection of the special category of data covered the practices and instrument application methods for medical data protection in Slovenia, Portugal, Germany, Ireland and Malta. The analysis of the specific proposals and recommendations on personal data protection in medical sector in Bosnia and Herzegovina are planned to be performed after the training. Participants of this training were civil servants from Ministry of Health of Federation of Bosnia and Herzegovina, Ministry of Health and Social Protection of Republic of Srpska, Ministry of Civil Affairs of Bosnia and Herzegovina, Bureau for Public Health of Federation of Bosnia and Herzegovina, Institute for Public Health of Republic of Srpska, Health Department of Brcko District and civil servants of the Personal Data Protection Agency in Bosnia and Herzegovina.

Raising awareness on the need to protect personal data

A total of 10 Press Releases in media and on the website of the Agency have been published in the reporting period with the aim of raising awareness of the citizens on the need to protect personal data. In this regard, on the website of the Agency a new link named "Actualities" has been established containing news and information on personal data protection worldwide.

On the 28 January, 2012, the Agency has, as previous years, organized the celebration of the European data protection day. On that occasion a press conference and "Open Door Day" have been organized and all interested citizens and representatives of the private and public sectors were invited.

In the aim of informing citizens, information flyers of the Agency on basic personal data protection principles have been distributed to municipalities in Bosnia and Herzegovina.

We have also created a brochure named "How to protect your personal data" in order to raise public awareness on personal data protection.

Media Cooperation

The Agency regularly informs media on its competences and activities and promotes its work and informs public regarding processing and protection of personal data. The Agency has usually answered and reported on time all media inquiries and through all available means of public communication: interview, written responses, press releases and publication of opinions on the official website of the Agency, as well as through the help desk. A total of 22 media inquires and 92 calls through the help desk of the Agency have been received in the reporting period.

The Agency has plans to continue unfinished activities in future period in order to achieve more significant progress in the area of personal data protection.

CROATIA / CROATIE

I. PERSONAL DATA PROTECTION

LAW AMENDMENTS

Since the Amendments to the Personal Data Protection Act (Official Gazette No. 130 of 11/16/2011, which entered into force on 11/24/2011) were adopted, the provisions of the Personal Data Protection Act are in its totality in accordance with the Directive 95/46/EC.

PROJECTS

During the reported period the Agency has participated in the next projects:

1. IPA 2007 Twinning project "Capacity Building of the Croatian Agency for Protection of Personal Data" (HR/2007/IB/JH/02)

- The 2nd Annex of the project was signed which extends the project for 2 extra months and foresees its culmination the July 28th 2012. New activities were incorporated to the project: programme for raising awareness of data protection officers, supply of advertising material and production of advertising spot.
- Held the workshop "Data Protection and Free Access to Information in the Croatian Legal Framework" where the target group were the courts administration.
- Organized and trained a special unit in the Ministry of Internal Affairs dedicated to the personal data protection in that ministry (over 600 attendants).
- Defined the procedures related to ISO 27001 standards for information security.

We can conclude that already now the results of this IPA 2007 Twinning project are even above the first expectations.

2. "Enhancing capacities of the CAPPD in the field of right of access to information" - project within the framework of the Dutch pre-accession bilateral assistance programme.

- Analysis of the current legal frame and its compliance with the EU legislation.

3. „Improving the Access to Information in Public Administration“- project within FFRAC 2010 and expecting for the EUD authorization, however, due to possible changes in the related legislation a postponement was recommended.

4. „Strengthen the Implementation of the New Freedom of Information Act“ - project within the framework of DIV/Reuniting Europe Programme

- 3 workshops were held dedicated to the information officers.
5. "Perception of the Data Protection and Privacy Issues by Children and Youth" - project held in the Leonardo da Vinci Programme framework
- A survey was organized among 6th grade elementary school, and 2nd grade high school children, on personal data protection perception and children and youth on-line privacy.
 - A termination of the programme was requested due to Hungarian partner renounced to the project.

Although the project was terminated before it was foreseen, the Agency has made the complete analysis of the leaded survey and this way fulfilled the predicted goals. The analysis of the result will be used for future activities related to child privacy protection.

6. „Strengthening the Role of Youth in Democratic Civil Society“- project which was applied to the UNDEF (The United Nation Democracy Fund) tender.
7. TAIX assistance:
- study visit to the Slovenian Information Commissioner,
 - study visit to the German Personal Data Protection Agency
 - workshop "Balance between the Right of Free Access to Public Information and Personal Data Protection in Media Reporting "
 - approved the visit of public interest and proportionality test expert
8. In the framework of the Lifelong Learning Programme Leonardo da Vinci, the Agency on 2012 together with its partners from Bulgaria, Czech Republic and Poland, apply to the project "Raising Awareness of the Data Protection Issues among the Employees Working in the EU"

INFORMATION SAFETY

- The Agency carried out the needed preparation activities for introducing Security Zone II, in compliance with the provisions of the Information Safety Act (Official Gazette 79/07)
- The Agency completed the activities to receive the ISO 27001 Certificate, understanding by that the incorporation of a administration system for information security. The certification of the Agency would indicate that it's ready for the

execution, administration, control, keeping and improving a documented ISMS within the Agency's labour activities

SUPERVISION

In the reported period the Agency has acted *ex officio* as well as according with the submitted requests for personal data protection

In this six-month period 126 data protection requests have been submitted to the Agency. The majority of them were related to: on-line personal data processing (web forums and sites, social networks, etc.), personal data processing with marketing purposes, legal acts execution and legal assignment, transfer of personal data, processing of personal data on association membership, and others.

Among the totality of the submitted protection requests, 44 were related to personal data processed by *Imenik d.o.o.*, a trade association from Zagreb, on its web site www.imenik.hr. The submitters remarked that there was publicly published the personal data of trade associations legal representatives without any legal basis. The same trade association was accused for publishing all the subscribed public telephone numbers in Croatia. Smaller number of requests was related the processing of hidden telephone numbers in the abovementioned website.

In the mentioned case, the Agency determined that the personal data of the trade association legal representatives was processed and published without legal basis and in discordance with the Personal Data Protection Act. Therefore, the Agency has forbidden *Imenik d.o.o.* such personal data processing and requested the deletion of the embraced personal data. Also, the Agency found the processing of the prepaid telephone numbers and related personal data in compliance with the Croatian Telecommunication Act. The Agency is still deducing if the secrecy of the hidden numbers was properly requested.

A certain number of personal data protection requests were submitted due to on-line publishing of personal data (social networks included), in such cases data deletion was requested by the submitters. However, in the cases when the domain is located outside Croatia, this Agency hasn't authority for such action.

It's important to remark the increasing number of requests for personal data protection regarding the marketing offers of insurance companies, prize game participation and association membership.

In the *ex officio* held cases and supervision of records delivery to the Central Register, the Agency requested to Personal Data Filing System Controller the delivery of records, and correction of the already delivered ones, in accordance with the legal provisions.

In the period this report refers to, the Agency enacted 5 decisions acting *ex officio* against Personal Data Filing System Controller, and 15 decisions and 32 opinions acting by the submitted requests.

According with the national laws, the decisions of this Agency can be revoked only by administrative complaint to the Administrative Court. In this period 4 of such processes have been started against Agency decisions, and that processes are still continuing. Also, the Administrative Court dismissed one complaint against an Agency decision.

Finally, the Agency has started 2 processes against Personal Data Filing System Controller and the responsible person at the Misdemeanour Court.

CENTRAL REGISTER

Personal Data Filing System Controller and Recorded Personal Data Filing Systems

From the next tables is appreciable the number of Personal Data Filing System Controllers and Records on Personal Data Filing Systems that have been recorded during the reported period, as well as the total figure.

Personal Data Filing System Controller

Status on 11/30/2011	Period	New Records	Total no. of Records till 05/18/2012
7.811	12/1/2011 05/18/2012.	476	8.287

Records on Personal Data Filing Systems

Status on 11/30/2011	Period	New Records	Total no. of Records till 05/18/2012
18.005	12/1/2011 05/18/2012.	1.602	19.607

PUBLIC RELATIONS, EVENTS AND SEMINARS FOR PDFS CONTROLLERS

Cooperation with Media

The Agency answered the enquiries frequently and reported timely throughout all the public information means: interviews, written answers, press releases as well as through its website. It's important to remark that the Agency answered press enquiries or held media presentations of the Agency's work 24 times.

Events and Seminars

Date	Activity	Target Group
01/26/2012	Seminar and Workshop Zagreb	PDFS Controllers
01/26/2012	„Open Doors Day“	Public
01/26/2012	Lecture „Privacy Protection and Free Access to Information in the Work with the Media“	Studenti VŠ „Kairos“
01/27/2012	Lecture and Additional Programme „Privacy Protection of Children“	Elem. School Matka Laginje
02/07/2012	Info-Point - Safe-Internet Day	Public, especially children
03/13/2012	Seminar and Workshop Slavonski Brod	PDFS Controllers
03/14/2012	Seminar and Workshop Sisak	PDFS Controllers
03/15/2012	Seminar and Workshop Karlovac	PDFS Controllers
05/09/2012	Workshop „Young Personal Data Filing System Controller“	Elem. School Matka Laginje

II. RIGHT OF ACCESS TO INFORMATION

In relation with the access to information right in this six-month period, the Agency has received 260 cases and has started 4 misdemeanour processes before the relevant court in compliance with the article 26th of the Right of Access to Information Act.

The Agency participated in the Partnership for Open Governance initiative for making an Action Plan. In the framework of the project „Strengthen the implementation of the new Freedom of Information Act“, the Agency actively took part of 5 workshops for information officers. The Agency has also organized, in cooperation with TAIEX, a workshop on “Balance between the Right of Free Access to Public Information and Personal Data Protection in Media Reporting“. With the support of TAIEX the Agency employees had a study visit to the Slovenian Information Commissioner on “Specific Topics Related to the Right of Access to Information in Public Administration“. Also, the Matra Flex project has started on the topic „Enhancing Capacities of the CAPPD in the Field of Right of Access to Information“.

The Report on the application of the Right of Access to Information Act for the year 2011 was composed, as well as the Report on Forming and Conducting the Overview of Signed and Executed Public Tender Contracts.

Finally, the since April 2012 the Agency is participating in the Working Group for Amending the Right of Access to Information Act.

CYPRUS / CHYPRE

The only major development in the field of data protection in Cyprus is that the amendment Directive 2009/136/EU of the e-privacy Directive 2002/58/EC was finally transposed into national legislation and therefore the Regulation of the Electronic Communications and Postal Services Law 112(I)/2004 was amended accordingly.

With regard to the Data Protection Law (The processing of Personal Data (Protection of Individuals) Law 2001) an amendment Law is before the House of Representatives and hopefully it will be finalized in June. Further information will be provided after the publication of the amendment Law in the Cyprus Official Gazette.

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

- In 2011 the Office applied in very concentrated way its supervisory powers on illegal video surveillance running within the meaning of the Act on the Protection of Personal Data.
- As a result of these Office's activities the situation in monitoring in the towns and transport was improved. Video surveillance using was strengthened in limits and on the basis of special laws.
- The Labor Code is primarily violated by the employers who monitor using video surveillance the employees in their workplace. That is why the Office initiated and has developed the cooperation with the labor inspectorates.
- As for video surveillance running in the residential buildings the Office elaborated the recommendation for housing cooperatives and residential units owners.
- In connection with developing of the Action Plan originated from the Government Resolution of September 14th 2011, which was adopted in context with an international initiative Open Government Partnership, the Office has actively participated in all negotiations coordinated by the Deputy Prime Minister and enforced essential amendment to the Act on free access to information with the aim to clarify the links to the Act on the Protection of Personal Data.
- In various contacts with the mass media staff the Office spread the knowledge of the Act on the Protection of Personal Data among the journalists and debated with them specific cases of its application in their work. Both sides, the Office and mass media representatives, expressed the interest to continue in this cooperation.
- In cooperation with the Polish supervisory authority (Biuro Generalnego Inspektora Ochrony Danych Osobowych) and Hungarian supervisory authority (Adatvédelmi Biztos, Parliamentary Commissioner for Data Protection and Freedom of Information) was established a publication – an aid for personal data controllers „Selected data protection issues. Guide for entrepreneurs“, supported by the European Lifelong Learning Programme Leonardo da Vinci (Education and Culture DG), which was published in Polish, Hungarian, English and Czech in 2011.
- In 2011 the yearly held competition for youth „My Privacy! Don't look, don't poke about!“ was focused on propagation of knowledge of problems connected with the use of Social Network, which threatens the privacy of its users.

ESTONIA / ESTONIE

- A. The legal regime that regulates access to payment default data is rather liberal in Estonia, but the legislature has imposed some restrictions on making lists of debtors public. An important precedent is the [Supreme Court decision made in December 2011](#), which confirmed the opinion of Estonian Data Protection Inspectorate that disclosing expired debt data forever is not permitted and that the deadline is 13 years.
- B. In January 2012 we published “Guidelines on the Use of Electronic Contact Details for Direct Marketing”.
- C. We may say that celebrating the Data Protection Day has become a tradition. On 27 January 2012 we organised a conference “Correcting Mistakes: Protecting Data of Minors”. The main topic was the role of educational institutions in awareness-raising with respect to what personal data is and why processing needs to be protected.

FINLAND / FINLANDE

The Parliament of Finland approved the 2001 protocol ETS No.181 and the required national law for incorporating the provisions into national law on 27 March 2012. Both instruments will be presented to the President of the Republic for approval and confirmation respectively in late June 2012.

The action of the Data Protection Ombudsman

1. Data Protection Day

The Data Protection Ombudsman did run a workshop on the theme of “What’s coming about in the security breach?”, in which was discussed about the potential risk of security breach to the citizens in reality, do we have right tools to react to it?

The Data Protection Ombudsman did also stage a press conference about the discovery of the workshop and allowed for discussion and questions concerning it and protection of personal data in general.

He also made on hand the material of data protection to children and the youth in the virtual Habbo Hotell.

2. The other action

The main emphasis in the action of the Data Protection Ombudsman has still been, in accordance with his goals, preventive operations. Aiming to have an influence on the public, he has focused on giving appropriate advice and guidance and integrating into working groups and committees which are significant in the field of data protection.

The office of the Data Protection Ombudsman has still had extensive co-operation with different interest groups. Various data protection steering groups has been operated in, among others, the sectors of public health care, social welfare, telecommunications and education.

GERMANY / ALLEMAGNE

Developments in the field of data protection at national level in 2011/2012

1. German Bundestag Study Commission on the Internet and Digital Society

In 2010, the German Bundestag decided to set up a study commission to look at the Internet and the digital society. 17 Members of Parliament and 17 experts have combined their efforts to study the issues in hand and are expected to submit their findings and recommendations by March 2013.

So far, the study commission has concluded four project groups. These are the project groups on data protection, media literacy, net neutrality and copyright. Further project groups are currently active, these being the ones dealing with democracy and the state, business, labour affairs and green IT, online access, structure and security, education and research.

The project groups dealing with interoperability, standards, open source; culture, the media and the public; international issues and internet governance and consumer protection are expected to take up work in June 2012.

The following interim reports and policy recommendations have so far been published:

- Interim Report on Data Protection and Privacy Rights ("Zwischenbericht zum Thema Datenschutz und Persönlichkeitsrechte") (15 March 2012)
- Interim Report on Net Neutrality ("Zwischenbericht zum Thema Netzneutralität") (2 February 2012)
- Interim Report on Copyright ("Zwischenbericht zum Thema Urheberrecht") (23 November 2011)
- Interim Report on Media Literacy ("Zwischenbericht zum Thema Medienkompetenz") (21 October 2011).

For further information - in the German language - concerning the study commission and the interim reports compiled by it please go to <http://www.bundestag.de/internetenquete/index.jsp>

2. Federal Government internet policy

The Federal Ministry of the Interior discussed the future of German internet policy with representatives from civil society, industry, research and administration during four consultations in 2010.

Discussions have focused on the issues of data protection and data security and have been summed up in 14 theses on internet policy to be found at <http://www.bmi.bund.de> The Federal Ministry of the Interior has taken various measures to implement these internet policy recommendations; it has, for instance, launched the Code for Social Networks, which is currently being drawn up.

In November 2011, the internet industry, at the initiative of the Interior Ministry, began to draw up pragmatic rules to protect users and consumers in social networks, led by the Voluntary Self-Regulation Body of Multi-Media Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, FSM), an organization which has already gathered practical experience with voluntary commitments.

The following enterprises take part: Facebook, Google, LinkedIn, Lokalisten, StayFriends, VZ Netzwerke, wer-kennt-wen.de and XING AG. This means that the most relevant national and international providers have been enlisted.

The Federal Government supports the efforts to elaborate the above-mentioned code, which is expected to be finalized in the last six months of 2012. The participating companies and the FSM have agreed to lay down voluntary commitments regarding i.a. the following issues:

- privacy by default
- data security
- transparency and controls for users
- concerns of younger users
- adequate risk management, e.g. efficient ways to report inadequate content
- user-friendly log-off processes and ways to delete user data
- right of non-users to determine the use of their data
- transparency with regard to the data stored.

3. Contest "Vergessen im Internet" (Forgetting and the Internet)

On 7 May 2012, the Federal Minister of the Interior, together with the German Academy for Technical Sciences (acatech; Deutsche Akademie der Technikwissenschaften), selected the winners of the contest launched in April 2011 to gather ideas on how to limit the shelf-life of internet content.

Pupils, students, businesses and private individuals had been invited to submit contributions in the three categories of "making users aware of risks", "manners and rules", and "technical forgetting solutions".

4. Draft Act to Regulate Data Protection in the Employment Sector

On 25 August 2010, the Federal Government adopted a Draft Act to Regulate Data Protection in the Employment Sector, which is currently going through the parliamentary process. This process is accompanied by a broad discussion by business and academia, interest groups and the general public.

5. Data Protection Foundation

The Federal Government is planning to set up a data protection foundation, which is

- to look at whether products and services comply with data protection needs,
- to enhance data protection education,
- to make users more aware of data protection measures which they can take to protect their data and
- to develop a data protection audit.

The plan is to set up the foundation as a non-profit and incorporated entity under public law. A total of 10 million euro has been earmarked for the foundation's assets in the federal budget.

Policy discussions are currently being held concerning the establishment of the Data Protection Foundation.

6. DE-Mail Act

On 3 May 2011 the Federal Government adopted an Act called "DE-Mail Act", DE being short for Deutschland, or Germany.

The Act seeks to make important security functions for the electronic exchange of messages user-friendly and thus accessible to a broad general public. These functions are, among other things, encryption, verifying the identity of communication partners, and making it possible to prove that a message has been sent or received – functions not available under the current mailing systems.

The new provisions and the technical guidelines governing DE-Mail have created the necessary framework conditions. DE-Mail has been realized and operated by accredited, mostly private, providers.

Potential DE-Mail providers may apply to the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) to be approved for the above-mentioned services. So far, Deutsche Telekom AG, United Internet (which provides web.de and GMX), Deutsche Post AG and the Mentana Claimsoft company have announced that they intend to provide De-Mail services.

7. The electronic identity card

On 1 November 2010, the new electronic identity card was launched in Germany. It enables card holders to prove their identity - safely and unequivocally – when using the internet or toll machines and other technical devices. The ID card chip can transmit the necessary data using secure connections as soon as the card holder authorizes such transmission by entering a PIN. Authorization certificates control which personal data may be transmitted to providers of internet applications and administrative services.

The Federal Commissioner for Data Protection and Freedom of Information was involved in the process of designing the new personal identity card from an early stage, and has acknowledged that it is privacy-friendly. Privacy-by-design played an important role. The EAC, BAC and PACE protection mechanisms, which have been applied in this context, are recognized world-wide in terms of data protection and rank top under IT security aspects.

Data stored on the new identity card can also be secured by what is known as "authorization certificates". To this effect, the "authority issuing authorisation certificates" (Vergabestelle für Berechtigungszertifikate, VfB), has been set up at the Federal Administration Office. Any enterprise, institution or authority wishing to access ID card data has to apply for the corresponding access rights. This authority will then check thoroughly whether or not applicants actually need the data for their business transactions. If not, authorization will be denied.

The federal Länder are responsible for making specific arrangements in order to manage the tasks arising from the law governing ID cards. This means that the identity card authorities must take measures to ensure the protection of personal data held or used by local authorities. That said, the Federal Ministry of the Interior makes every effort to assist these authorities and has given them IT security guidelines developed by the Federal Office for Information Security especially tailored to their needs.

8. Amendment of the Telecommunications Act

On 10 May 2011, the Act to Amend the Telecommunications Act entered into force. The aim is to adopt new information and transparency rules (for instance regarding the location of persons)

and to thus improve data protection provisions. The overarching aim is to better protect sensitive data and to strengthen the legal position of those using telecommunication services.

9. Cloud computing

The Federal Ministry of Economics and Technology has launched a technology programme called “Trusted Cloud”. In the next three years, 14 innovative, secure and legally robust cloud solutions will be developed and tried in various application fields. At the same time, the Ministry of Economics has set up the “Trusted Cloud Competence Centre”, which brings together several working groups to address cross-cutting issues. The working groups are coordinated and accompanied by experts. One working group deals with the legal framework concerning cloud computing (including data protection).

10. IT summit

The mobile internet entails additional data protection challenges e.g. because it can easily be used to locate persons and because of the growing use of social media. In 2011, several working groups of the national IT summit looked at how to meet these challenges in a process involving federal ministries, business representatives, data protection commissioners and consumer associations. As a first step, a list of tips for users concerning has been compiled, which were published at the IT summit on 6 December 2011.

ICELAND / ISLANDE

According to Art. 33 of Act no. 77/2000, on the Protection of Privacy as regards the Processing of Personal Data, certain processing of general or sensitive personal data may not begin until it has been examined by the Data Protection Authority (DPA) and approved of, by the issuing of a special permit, if it is likely to present specific risks to the rights and freedoms of data subjects. Likewise, according to Art. 15 of Act no. 74/1997, on the Rights of Patients no. 74/1997, the DPA is authorized to give access to information contained in clinical records, including biological samples, for the purposes of scientific research. A new bill is now being drafted regarding scientific research. This new bill assumes that the DPA will not deal with the aforementioned permits, regarding access to information contained in clinical records, but instead by the National Bioethics Committee (NBC), which is appointed by the minister of welfare, and other bioethics committees for certain health establishments. The DPA however has proposed that these committees will send the DPA a summary of issued permits so that the DPA can decide, based on these summaries, if there are occasions for further examination of individual cases/researches.

It is also worth mentioning that there has been a significant increase in the DPA's case handling parallel to cut backs in budgetary resources. As an example there was a 16% increase in case handling between 2010 and 2011 whereas during the same time frame budgetary resources were cut back. Case-handling has developed progressively over the last 10 years and in 2011 newly registered cases were 1.397 in total. During this expansion the DPA has mostly had the same number of employees - the executive director, four lawyers and a financial officer. It is evident that the DPA will not be able to manage the tasks it is entrusted according to law, in a satisfactory way.

IRELAND / IRLANDE

On 21 December 2011 the Office of the Data Protection Commissioner published its Report on the outcome of its audit of Facebook Ireland (FB-I). The Report provides a comprehensive assessment of Facebook Ireland's compliance with Irish Data Protection law and by extension EU law in this area. Facebook Ireland has responsibility for all Facebook users outside of the USA and Canada.

The audit found a positive approach and commitment on the part of FB-I to respecting the privacy rights of its users. Arising from the audit, FB-I agreed to a wide range of "best practice" improvements to be implemented during the first 6 months of 2012 with a formal review of progress to take place in July 2012.

The Audit was the most comprehensive and detailed ever undertaken by the Office of the Data Protection Commissioner.

The Report records significant recommendations and commitments from Facebook Ireland in relation to:

- a mechanism for users to convey an informed choice for how their information is used and shared on the site including in relation to Third Party Apps
- a broad update to the Data Use Policy/Privacy Policy to take account of recommendations as to where the information provided to users could be further improved
- transparency and control for users via the provision of all personal data held to them on request and as part of their everyday interaction with the site
- the deletion of information held on users and non-users via what are known as social plugins and more generally the deletion of data held from user interactions with the site much sooner than presently
- increased transparency and controls for the use of personal data for advertising purposes
- an additional form of notification for users in relation to facial recognition/"tag suggest" that is considered will ensure Facebook Ireland is meeting best practice in this area from an Irish law perspective
- an enhanced ability for users to control tagging and posting on other user profiles
- an enhanced ability for users to control their addition to Groups by friends
- the Compliance management/Governance function in Dublin which will be further improved and enhanced to ensure that the introduction of new products or new uses of user data take full account of Irish data protection law.

The report is available on the Data Protection Commissioner's website: <http://dataprotection.ie>.

ITALY / ITALIE

Regulatory Developments

Amendments were made to the Data Protection Consolidated Code by two separate Acts: namely, Act 214/2011 of 22 December 2011 modified the definitions of “personal data” and “data subject” in order to exclude legal persons from the scope of application of the relevant provisions (the definitions now read as follows: “ ‘personal data’ shall mean any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number;” “ ‘data subject’ shall mean any natural person that is the subject of the personal data”); Act 35/2012 of 4 April 2012 simplified the requirements applying to the processing of personal data via electronic tools by eliminating the need for data controllers to draw up the so-called “Security Policy Document” (listing the specific arrangements and policy implemented to ensure data security in line with the law) with regard to the processing of sensitive and judicial data.

It should also be pointed out that transposition of directive 2009/136/EC (which amended the e-privacy directive 2002/58) is about to be finalized along with that of directive 2009/140/EC; it is expected that the regulatory text will be modeled closely after that of both directives.

Main Issues Addressed by the DPA

(April 2012) Tax Data and Privacy: The DPA gave its opinion on the draft ruling of the Director of the Italian Revenue Office specifying the modalities for the transmission by Italian financial institutions of data on bank accounts with the aim of countering tax evasion. Given the main criticalities in question, the Italian DPA laid down the technological and organizational measures required to enhance security and to bring the processing into line with data protection legislation. In doing so, the Garante took into consideration the entire data-cycle, that is, from the transmission of data by banks (also through so-called ‘authorized intermediaries’) to the Taxpayers’ Register (Anagrafe Tributaria) via the connection channel ‘Entratel’, whose security should be improved, to the storage, access to and deletion of such data (i.a., setting forth appropriate data retention periods).

(February 2012) RFID Technology to Monitor Access to Restricted Traffic Areas: The DPA authorized a municipality to implement an RFID-based system to record the flows of trucks and similar utility vehicles in a restricted traffic area. The system is meant to prevent such vehicles from driving in the area for longer than is permitted by the applicable municipal regulations and should facilitate imposing the relevant fines. RFID tags installed on the access-enabled vehicles will be read by devices located at the entrance/exit points. As well as requiring adequate information to be provided to the drivers, the DPA ordered that the data recorded in the system should be erased once the vehicle had left the restricted traffic area if no breach of the relevant regulations was detected; if this was not the case, the timestamp and related information would be associated with the driver’s personally identifiable information and used for imposing the applicable fines. It could be established that no tracking of the routes followed by the vehicles was performed by the system, which accordingly did not give rise to any monitoring of employees’ (drivers’) performance.

(January 2012) Health-Related Blogs and Websites: The DPA issued guidelines to enhance the security of health-related information posted on blogs and similar forums dealing with medical issues. A specific “risk notice” will have to be provided by the managers of such blogs/websites to all visitors in order to draw their attention to the risk of their being identified along with the

respective disease(s) if they enter sensitive data jointly with their personally identifying information. The notice is also aimed at informing visitors of the measures required to protect their privacy both during registration (if the website/blog requires registration) and when entering data in the web area(s) they can visit. Specific mention should be made of the indexing arrangements applying to the blog/website (i.e. whether the information posted may be crawled by external search engines). The DPA also suggested that users should be directed to the “Risk Notice” via a clickable icon posted on the home page of the blog/web site.

(December 2011) Telemarketing and Silent Calls: Specific instructions were given to a major utility company in Italy as for the telemarketing activities performed (by way of outsourced services) with the help of ad-hoc software for the allocation of operator-assisted calls. The DPA required that the software (and systems) used by the company should be designed in a privacy-compliant way, i.e. that the making of repeated (at times sequential) “silent calls” (i.e. calls where a person hears nothing on the end of the line on answering the phone and has no means of establishing whether anyone is at the other end) should be prevented. To that end, call repetition should be barred by the system (in case of an initial silent call) for a period of at least thirty days.

LATVIA / LETTONIE

During the period under the review, Data State Inspectorate of Latvia participated in the consideration and discussion process related to the initiative of European Commission regarding the comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. There has been a major interest from the general public and different public and private sector institutions regarding this reform. Thus Data State Inspectorate of Latvia has been collaborating with the Ministry of Justice in order to draw a draft position of the Republic of Latvia on this issue. In fact, the discussion of this reform has been launched on the Data Protection Day of this year that was celebrated on 30 January 2012.

In order to foster mutual cooperation, Data State Inspectorate of Latvia participated at the first meeting of the three Baltic States where an agreement was achieved to launch each year common control activities. Furthermore a common draft project was elaborated by the three Baltic States regarding the children privacy protection within the online environment and it has been submitted by the Ministry of Justice of Latvia to the European Commission.

As in previous years, the office attended data protection meetings both at European, international and national level, as well as meetings of the Working Group established under the article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as the Joint Supervisory Body meetings of Europol, Schengen and Customs.

Within the year 2011 there have been 257 written complaints received in Data State Inspectorate of Latvia, from those the main complaints were related to:

- 1) transfer of personal data to third parties within the debt collection process;
- 2) disclosure of information regarding the debt for public facility services to the third parties;
- 3) disclosure of personal data on the internet (the number of cases thus has been increased where international cooperation has been necessary);
- 4) registration of natural persons as the employees at the State Revenue Service and as the members of the company's board at the Register of Enterprises without the consent of this person.

Regarding the 47 investigated cases Data State Inspectorate applied administrative penalties regarding the violation of Personal Data Protection Law – 24 warnings and in 23 cases fines have been applied.

One of the main priorities of the current year is the foreseen Schengen evaluation visit that would take place in Latvia in October this year regarding the application of Schengen *acquis* in the field of data protection. Regarding this issue there is a discussion going on regarding the possible amendments to the [Law On Operation of the Schengen Information System](#).

Regarding the raising awareness of the general public, Data State Inspectorate of Latvia regularly provides mass media on different issues related to the personal data protection. It has also been foreseen to elaborate two recommendations this year – regarding personal data protection within the labor relations and data security.

LIECHTENSTEIN

The relatively short period since the last plenary meeting saw the following main activities:

As every year, at the occasion of the **European Data Protection Day** the Liechtenstein Data Protection Authority (DPA) organised a public event at the University of Liechtenstein on 26th January 2012. The topic chosen was “online behavioural advertising / online targeting”. After an event on search engines and one on social networks in the previous years, this was the third event on Internet related topics. The reason for the choice of the topic lay in the change of the European regulatory framework (Directive 2009/136/EC).

The DPA was involved in the drafting negotiations with the United States of America on an agreement on preventing and combating serious crime including an automated exchange of fingerprints and DNA-data (“**Prüm-like Agreement**”).

Furthermore, the DPA has finished a **control** in the area of data retention. It established a report which was submitted to the National Police. Following a complaint, it started a control in the health insurance sector and with the Department of Statistics.

Moreover, the DPA published an **information sheet** concerning **Schengen** and in particular the rights of data subjects.

Finally, it published **guidelines** on technical and organisational measures to protect data and updated the guidelines on processing on the one hand, and on disclosing data on the other.

LITHUANIA / LITUANIE

LE TRANSFERT DE DONNEES A L'ETRANGER

L'inspection nationale de protection des données personnelles a reçu l'enquête d'un responsable du traitement sur transfert de données à caractère personnel des actionnaires et des clients à l'entreprise de la Russie. L'inspection a été saisie en demandant, est ce que tel transfert ne contredira à la loi de protection juridique des données personnelles. La demande de l'entreprise de la Russie était sur la base de l'ordonnance du premier ministre de la Russie. En réponse à l'enquête ladite, L'inspection a noté bien que la Convention pour la protection des personnes à l'égard du traitement automatisé des données a caractère personnel est signée par la Russie, mais ce pays ne l'a pas ratifiée, aussi la Russie n'est pas reconnue comme le pays assurant un niveau de protection adéquat.

PROCÉDURE D'ÉVALUATION EN VERTU DES DECISIONS 2008/616/JAI ET 2008/615/JAI DU CONSEIL

Mise en œuvre la décision N° 2008/615/JAI du Conseil le 9 novembre 2011 le Gouvernement de la République de Lituanie a adopté la Résolution N ° 1324. Cette résolution a adopté la description de la procédure de l'échange transfrontalier de données ADN, de données dactyloscopiques, d'immatriculation des véhicules, leurs propriétaires et gestionnaires et d'informations liées aux grands événements transfrontaliers ou à prévenir les infractions terroristes.

Procédure d'évaluation à la Lituanie en vertu des décisions 2008/616/JAI et 2008/615/JAI du Conseil est commencée l'année dernière. En 2011 visite d'évaluation a eu lieu sur l'échange automatique de données génétiques et dactyloscopiques. Cette année, en Juin visite d'évaluation prévue à la Lituanie en vertu des décisions du Conseil ci-dessus pour l'échange automatique de données d'immatriculation du véhicule, leurs propriétaires et les gestionnaires. L'inspection nationale de protection des données personnelles participera également à la visite d'évaluation.

LUXEMBOURG

Du 3 au 4 mai à Luxembourg

Conférence annuelle des autorités européennes à la protection des données

Du 3 au 4 mai 2012, le Luxembourg accueille la conférence de printemps (« Spring Conference ») des commissaires européens à la protection des données à l'amphithéâtre de la Cour des comptes européenne.

Cette année-ci, la Commission nationale pour la protection des données (CNPD) organise cette conférence, qui a lieu chaque année dans un pays différent. Elle réunit les délégués des autorités de 38 pays, ainsi que les représentants de la Commission européenne, du Conseil de l'Europe et de l'OECD.

Le thème de la conférence s'intitule « *La réforme de la protection des données européenne confrontée aux attentes !* ».

Dans une première table ronde, présidée par le Superviseur européen Peter Hunstinx, sont notamment intervenus le commissaire fédéral allemand Peter Schaar et son collègue britannique Christopher Graham au sujet des défis et enjeux majeurs de la récente proposition législative de la Commission européenne.

Si les travaux de la conférence ont principalement porté sur la protection des données en Europe et en particulier dans l'Union européenne, la réflexion des commissaires a également été menée en tenant compte du contexte de l'évolution en matière de « privacy » dans d'autres parties du monde. La participation de David Vladeck, directeur de la Federal Trade Commission (FTC), a particulièrement retenu l'attention puisqu'il a exprimé un point de vue transatlantique sur les nouvelles dispositions proposées par la Commission européenne.

Le ministre François Biltgen, en sa double qualité de ministre de la Justice et ministre des Communications et des Médias, a commenté les enjeux majeurs, notamment pour le Luxembourg en tant que data hub. « *L'économie numérique, nouveau pilier économique et priorité pour le gouvernement, a besoin d'un cadre légal stable et digne de confiance* », a noté le ministre.

Il a réitéré la volonté politique en faveur d'un cadre équilibré. « *Dans sa politique visant le développement rapide et diversifié de nouvelles technologies, le Gouvernement prête une attention particulière à la protection de la vie privée et des libertés individuelles, permettant ainsi de tirer le meilleur parti du progrès technologique tant pour les entreprises innovantes que pour les citoyens.* »

Lors des différentes séances, les commissaires débattent en particulier du renforcement des droits des utilisateurs de services sur Internet, notamment dans le contexte du cloud computing et des réseaux sociaux. Des tables rondes spécifiques portent aussi sur la simplification des



COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

obligations administratives des acteurs en faveur d'une plus grande responsabilisation, de l'évolution du rôle renforcé des autorités de contrôle, de la protection des données dans le domaine de la police et de la justice, ainsi que de la modernisation des autres instruments juridiques internationaux (Convention 108 du Conseil de l'Europe et lignes directrices de l'OCDE).

La Vice-présidente de la Commission européenne, Viviane Reding, Commissaire européenne à la Justice, a noté dans son message adressé aux participants : *« La réforme de la protection des données, présentée par la Commission européenne, établit un seul et même ensemble de règles de protection des données fortes qui assurent davantage de contrôle sur leurs données à nos citoyens tout en rendant plus aisé aux entreprises d'être en conformité pour tirer profit du Marché Unique. Mais une législation uniforme, ce n'est pas suffisant. Nous avons aussi besoin que quelqu'un veille à ce que ces règles soient appliquées partout à travers l'UE, et partout de la même façon. C'est pour cela que notre réforme renforce considérablement le rôle des autorités de contrôle national et harmonise leurs missions et pouvoirs de façon à ce qu'elles puissent faire de ces règles une réalité effective pour les 500 000 citoyens européens et les entreprises. »*

Le Président de la CNPD, Gérard Lommel, a souligné l'importance d'une modernisation du cadre juridique de la protection des données *« pour rendre la législation plus efficiente, plus claire et simple à la fois pour la mise en conformité des multiples acteurs qui collectent de plus en plus de données des citoyens ou consommateurs et pour les individus de façon à leur conférer davantage de transparence et de contrôle et de leur faciliter l'exercice de leurs droits, en particulier dans l'environnement numérique. »*

Il a par ailleurs annoncé qu'« ensemble avec ses collègues des autorités de protection des données à travers l'Europe, la CNPD se prépare à mettre en œuvre les prérogatives renforcées prévues dans le projet de l'UE, à intensifier aussi bien son dialogue avec les acteurs, que sa guidance et ses contrôles et à mettre à profit les outils innovants (Privacy impact assessments, Chargés désignés, Notifications de violations de sécurité). »

Luxembourg, le 3 mai 2012

Communiqué par la Commission nationale pour la protection des données
41, avenue de la Gare
L-1611 Luxembourg
Tél : 26 10 60 – 1
Fax : 26 10 60 – 29
E-mail: info@cnpd.lu
Internet: <http://www.cnpd.lu>



Assurer la protection des données dans un monde globalisé

La CNPD et le SnT concluent un contrat de partenariat pour effectuer des recherches conjointes sur la protection des données personnelles

La Commission Nationale pour la Protection des Données luxembourgeoise (CNPD) et le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg ont conclu un contrat de partenariat stratégique. Les deux partenaires lanceront un programme commun de recherche analysant les nouveaux développements de la législation en matière de protection des données, les défis technologiques tels que le cloud computing, les répercussions pour le site économique luxembourgeois et les solutions pour assurer la protection de la vie privée dans un monde globalisé.

La protection des données personnelles joue un rôle de plus en plus significatif tant à l'échelle internationale qu'au Luxembourg. La conformité à la législation en la matière devient d'autant plus importante pour les différents acteurs traitant des données. Compte tenu de l'évolution rapide des technologies de l'information et de la communication (TIC) et de la réglementation dans ce domaine, les sociétés privées et les pouvoirs publics ont besoin d'un savoir-faire juridique et technique particulier afin de garantir que leurs activités répondent aux requis des lois en vigueur. La coopération entre la CNPD et le SnT sur le plan scientifique contribuera par son analyse conceptuelle et l'identification des aspects critiques à une approche approfondie et orientée vers l'avenir qui permettra d'assurer et d'améliorer la protection des données. Une attention particulière sera attachée à l'incidence des évolutions constatées sur les acteurs du site luxembourgeois.

En tant qu'autorité de contrôle, la CNPD est chargée de vérifier la légalité des traitements des données à caractère personnel des acteurs privés et publics. Elle s'occupe des demandes et plaintes des citoyens et avise les projets de loi. Lors de ses appréciations et investigations, elle se penche sur des questions juridiques et techniques. Le SnT mène des recherches scientifiques dans le contexte des services TIC tels que les réseaux de communication et les systèmes logiciels pour en améliorer la sécurité et la fiabilité et afin de renforcer la confiance des utilisateurs en ces services. La conformité à la législation sur la protection des données constitue souvent un élément essentiel des différents projets au SnT. Dans ces domaines, la CNPD et le SnT entendent réunir leur savoir-faire dans le cadre de leur partenariat stratégique.

Il importe d'avoir une compréhension rapide de la future législation européenne dans le domaine de la protection des données et d'en analyser les répercussions. Si cette législation correspondait bien à l'état de l'art en 1995, elle requiert aujourd'hui une refonte face à l'essor de nouveaux services en ligne tels que les réseaux sociaux. Dans ce contexte, le cadre législatif existant est actuellement réexaminé. La mise en œuvre de ces règles modernisées nécessitera, outre leur transposition en droit luxembourgeois, des travaux de recherche sur les répercussions qu'elles auront à la fois sur l'utilisation des données à caractère personnel et sur le travail des autorités de contrôle.

Un autre point d'intérêt commun concerne l'harmonisation du cloud computing et de la confidentialité des données. L'utilisation de plus en plus fréquente du cloud computing pour traiter les données à caractère personnel soulève des problèmes juridiques et techniques. La combinaison des compétences interdisciplinaires respectives de la CNPD et du SnT améliorera la compréhension des aspects techniques et réglementaires du cloud computing et de sa portée particulière pour le Luxembourg.



« Au cours des dernières années, de nouveaux services tel que Google Street View, mis en oeuvre dans un délai assez bref, ont constitué de réels enjeux pour le cadre législatif actuel et ont exigé une réponse rapide sur la manière de traiter ces services », déclare Prof. Björn Ottersten, directeur du SnT. Gérard Lommel, président de la CNPD ajoute que « notre programme de recherche commun répondra à ces questions fondamentales de la protection des données dans un environnement technologique moderne. Nos résultats contribueront à sensibiliser le public et aideront à définir des solutions 'made in Luxembourg' qui pourront servir d'exemples pour faire face aux nouveaux défis dans ce domaine dès le début ».

A propos du SnT

Créé en 2009 par l'Université du Luxembourg, le SnT est une plate-forme de recherche de renommée internationale qui, avec des partenaires externes, agit en sorte que le Luxembourg devienne un centre européen d'excellence et d'innovation en matière de systèmes et services TIC (Technologies d'information et de communication) sécurisés, fiables et dignes de confiance. Pour exercer une certaine influence, une approche interdisciplinaire de la recherche est essentielle, en tenant compte non seulement des aspects techniques, mais également des questions commerciales, humaines et légales. Le SnT propose une plate-forme d'interaction et de collaboration entre les chercheurs universitaires et les partenaires extérieurs.

www.uni.lu/snt

A propos de la CNPD

La CNPD a été instituée par la loi du 2 août 2002 pour vérifier la légalité des traitements de données personnelles et assurer le respect des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée. Elle émet des recommandations, avise des projets législatifs et mesures réglementaires, reçoit et examine les plaintes et demandes des citoyens de vérification de la licéité d'un traitement et approuve les codes de conduite sectoriels. Comme autorité de contrôle, elle dispose d'un pouvoir d'investigation conséquent et peut prendre des sanctions administratives ou saisir la justice. Sa mission s'étend également à assurer le respect des dispositions de la loi du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques, ce qui inclut les nouvelles technologies de l'information et de la communication et Internet.

www.cnpd.lu

Luxembourg, le 17 novembre 2011

Communiqué par la Commission nationale pour la protection des données

41, avenue de la Gare

L-1611 Luxembourg

Tél. : 26 10 60 – 1

Fax : 26 10 60 – 29

E-mail: info@cnpd.lu

Internet: <http://www.cnpd.lu>



COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

MALTA / MALTE

Protection Field since the 27th meeting of the T-PD

During the first months of 2012 to date, the Office received a total of twenty-five (25) complaints, where citizens felt their privacy was being threatened and therefore resorted to a remedy before the Information and Data Protection Commissioner (Commissioner). The most common subjects of these complaints referred to unsolicited communication via e-mail or text messages and disclosure of personal data without the data subject's consent. As part of the investigation of a number of the complaints received, this Office conducted inspections of the relevant data controllers in order to ascertain the veracity or otherwise of the alleged facts made in the respective complaints. So far this year, there has only been one case wherein one of the parties felt aggrieved by the decision of the Commissioner and in terms of article 49(1)¹ of the Act, filed an appeal before the Data Protection Appeals Tribunal. The case is scheduled for its first hearing before the Tribunal, in June.

Apart from complaints, during this period the Office also received several queries both by email and phone on the interpretation of data protection legislation. The queries received via e-mail amount to fifty-two (52) to date and on average the Office receives around five (5) queries per day over the phone. In particular the queries received relate to the notification obligation as imposed on data controllers that process personal data and the rights of the data subjects in particular the right of access. Other general queries dealt with the processing of personal data for research purposes, the filming and taking of photos in public places and the model contractual clauses. Data controllers also submitted queries concerning the introduction of tracking devices and the installation of CCTV camera systems.

The Office has an obligation to promulgate data protection awareness for the benefit of the citizen and various sectors and data controllers in general. In the light of this obligation, continuous work is undertaken. In particular during the period under review this Office continued with its participation on a radio program on the national station with the aim of discussing various topics in relation to the right of privacy. The listeners are given the opportunity to call during the program and ask questions about any problems or any circumstances where they felt that the right of privacy may have been impaired. Positive feedback is to date registered from this awareness initiative. Presentations were also delivered to data controllers with the objective of further raising awareness and in order to involve the key players in the evolution of the data protection culture. In particular two of such presentations were delivered to the 'Armed Forces of Malta' and the 'Malta College of Arts, Science and Technology'.

During the period under review the Office attended data protection meetings and conferences at European level as well as meetings of the Working Group established under article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In view of the upcoming Schengen evaluation, scheduled to be carried out in July 2012, this Office commenced with the necessary preparatory work intended to gear up for the peer review which shall be carried out by a team of European data protection experts. A technical team from this Office carried out two onsite inspection visits at the Embassy and Consular offices of Malta in Moscow and Cairo. The scope of the inspection visit was to assess the processing of

¹ "Any person aggrieved by a decision of the Commissioner shall have the right to appeal in writing to the Tribunal within thirty days from the notification to him of the said decision."

personal data undertaken by both missions in the process of issuing visas for third country nationals. The visit was also carried out with the objective of reviewing certain established procedures in the light of the requirements deriving from the provisions of the Data Protection Act and other legal instruments. A training session on data protection awareness was also delivered to members of staff to create awareness on the privacy rights citizens enjoy under the Act, the relative VIS regulations and the Schengen Convention in relation to the issuing of visas.

MONACO

Ci-après, les développements législatifs et réglementaires intervenus en Principauté de Monaco, dans le domaine de la protection des données, depuis la dernière session plénière :

- L'Ordonnance Souveraine n°3.717 du 28/03/2012 modifiant l'Ordonnance Souveraine n°765 du 13 novembre 2006 relative à l'organisation et au fonctionnement de la Direction de la Sûreté Publique précise les missions de la Direction de la Sûreté Publique et contient des dispositions relatives aux traitements d'informations nominatives mis en œuvre dans le cadre desdites missions. Ce texte introduit une obligation de traçabilité des accès aux dits traitements et de conservation pendant 10 ans des dits accès. Il généralise le droit d'accès indirect pour les traitements de police.
- L'autorité de contrôle a adopté les recommandations suivantes, lesquelles sont accessibles sur son site Internet www.ccin.mc : traitement des documents d'identité officiels- rappel des principes européens applicables aux traitements automatisés ou non d'informations nominatives- dispositifs de vidéosurveillance dans les immeubles d'habitation.
- La Principauté demeure dans l'attente de la décision de la Commission européenne quant à la demande d'adéquation introduite en novembre 2009.

MONTENEGRO

So far, the Agency has delivered three work reports to the Parliament (two regular annual ones and one interim report – for the period of six months). The report for 2011 received support of all members of the competent parliamentary Committee for Human Rights.

In Montenegro, the awareness that personal data protection is equally important as other human rights is still not high enough. Mass violations of rights have not occurred but individual cases are obvious and they mostly occur as the consequence of not being familiar enough with the legislation or its incorrect application.

State in the field of personal data protection is not on a satisfactory level both formally and factually.

The Agency performs supervision in accordance with the Personal Data Protection Law, through its inspectors authorised to carry out supervision affairs. Agency has managed to increase the awareness level on the need to protect personal data. It is evident that an increasing number of entities and data subjects are contacting the Agency by asking for opinions, approvals, explanations and also requests for the protection of rights. All of this indicates to the fact that the trust in the Agency, as independent institution, is increasing,

Higher level of personal data protection is noted, also through the number of submitted records on filing systems controllers. **The number of records** delivered to the Agency in 2011 was **462** and they were delivered by 120 controllers. Considering that Montenegro has 600 thousand citizens, we believe that this number is a good indicator of the Agency's quality work and we point out that the trend of record delivery is continued in this year as well.

This effect was achieved through the campaign of the Agency consisting of sending circulating notifications to warn the controllers of the provisions of the Law and the obligation to deliver records. In addition, a specific education is carried out through inspection supervision resulting in supervised entities carrying out their obligation noted down in the record on supervision i.e. among other things, by delivering their existing records on filing systems.

We would like to state that the previous year, regarding inspection supervision, was marked by a high level of cooperation of controlled entities, which is certainly a good thing from the perspective of the Agency. However, the cause for worry is the lack of knowledge of provisions in this area of a majority of controllers. Majority of them are still investing very little efforts to comply with the existing legislation.

In 2011, the supervision focus was also placed on video surveillance. During the process of controlling the introduction and use of video surveillance, it was noted that this manner of personal data processing is used massively and mainly contrary to the provisions of the Law, disproportionately and to a large extent. Degree of risk of such unlawful personal data processing is increasing, freely said, on a daily basis.

The basic issue regarding video surveillance concerned the following: the lack of Decision of the responsible person of the entity performing video surveillance; failure to display public announcement on video surveillance; lack of opinion of the union representative regarding video surveillance in the working premises where there is an objective need for it; carrying out video surveillance in a larger space compared to the space of the surveillance entity as well as

video surveillance in the part intended for employees or guests violating privacy without a legal basis.

The Agency has contributed in raising awareness on personal data protection, above all by performing significant supervisions, such as the supervision of mobile operators and Police Directorate concerning personal data protection, regarding the delivery of lists of phone calls and SMS messages. We believe that the practice until the Decision of the Agency was adopted was not in accordance with the Constitution of Montenegro, international treaties signed and ratified, and therefore, it must be changed in accordance with the existing legal order.

Progress can certainly be seen in practice because the Police Directorate and operators have complied with the Decision of the Agency, by only using a court order to obtain data from telecommunication traffic, list of phone calls and SMS and data from base stations. This practice, until the amendments to the Criminal Procedure Code are adopted which should contain provisions compatible with European standards, guarantees personal data protection in the part concerning legal basis for collection.

Irregularities noticed in a large number of supervisions concern personal data processing to an extent larger than necessary to achieve the purpose of processing, as well as inadequate personal data protection.

Agency, on the other hand, invested great efforts to present itself to professionals and amateurs by offering protection to citizens in all situations when they have suspicions that their personal data are inadequately processed or protected.

In the previous practice, we have recognised situations which present the most dangerous risks in the area of personal data protection in Montenegro, therefore, the Agency will focus its special attention to such phenomena. In addition to the previously mentioned, violation of citizens' privacy is done also via direct marketing so activities in this area is a great challenge. We are all witnesses that direct marketing, as an activity enabling the possibility of offering products and services or the communication of certain news via post, phone or other direct means to potential customers or buyers of these product or services, is present in our country. It is very often that we receive various information and offer to our contact addresses, phone or electronic without our consent being given to such data processing.

The application of new IT and communication technology enables a rapid progress of society, but besides its positive side it also has a negative one. By collecting the data on consumers, companies are cleverly adjusting their services or products to their needs thus ensuring larger profits. Therefore, every citizen must be careful to whom and why he is giving his personal data i.e. they must balance the benefit they are obtaining and possible harm from the abuse of data for the processing of which they gave their consent by filling in the application form.

We believe that the citizens still are not fully familiarized with their right to personal data protection, which is why, in addition to training the employees of the Agency as our primary obligation, we will continue educating the controllers and citizens, so that they contact the Agency in a larger number. We have the impression, from the requests submitted, that the citizens have indicated problems in data processing in various areas, from the circumstances of personal data processing without the consent of the data subject, processing scope which is larger than necessary, duration of processing, erasing personal data, etc.

Agency for Personal Data Protection is the beneficiary of the Twinning Project under the title "Implementation of the Personal Data Protection Strategy in Montenegro". Its implementation period is 15 months. The Project is now at its final stage. The short-term experts of this project have provided great assistance to our employees in their daily work and they assisted in the education of controllers by organising trainings.

Draft Law on amendments to the Personal Data Protection Law is in Parliamentary procedure and it is harmonized with international standards, particularly the Directive 95/46/EC. Adoption of the new Law is expected by the end of the first regular meeting of the Parliament of Montenegro which ends by the end of July.

The Agency has, in cooperation with the short-term experts of the Twinning project, drafted the analysis of 15 Laws that need to be harmonized with the Personal Data Protection Law and identified a significant number of other laws whose harmonization should be done in the future.

NORWAY / NORVÈGE

1. INTRODUCTION

In the following we will present an update on the major legal developments in Norway concerning personal data protection since the 27th meeting of the T-PD.

2. AMENDMENTS OF THE PERSONAL DATA ACT

The 27th of March 2012 the Norwegian Parliament adopted amendments of the personal data act. The amendments entered into force the 20th of April 2012.

The amendments ensure an increased protection of children's personal data, a better balance between data protection and the freedom of expression and a modernized approach to television monitoring. The amendments also simplify the scheme on licenses to handle personal data.

Before the said amendments processing of personal data solely for artistic, literary, journalistic, including opinion-shaping purposes was excluded from the scope of the personal data act. In the amendments of March 2012 the wording "including opinion-shaping" was removed from the legal text. The aim of the amendment was to clarify the scope of the exemption, and to ensure that the exemption was not given a too broad interpretation.

A new provision that provides for an increased protection of children was included in the personal data act. The provision states that personal data relating to children cannot be processed in an irresponsible manner. The provision gives the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child. The background for the introduction of this provision was alarming examples of adults violating children's right to protection of their personal data, and the realization that the technological development increases the risk of personal data about children being spread on the Internet.

POLAND / POLOGNE

1. Data protection law - change of law!

On **1 January 2012** new legal provisions having significant influence on personal data protection entered into force.

It needs to be emphasised that the **provisions of the Act of 29 August 1997 on the Protection of Personal Data** (Journal of Laws 2002 No. 101, item 926 with amendments) **were amended**. The changes were introduced by the Act of 16 September 2011 on exchange of information with law enforcement authorities of Member States of the European Union (Journal of Laws No. 230, item 1371), which entered into force on 1 January 2012, which implements Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Moreover, **on 31 December 2011 Art. 7a para. 2 of the Act of 19 November 1999 Economic Activity Law was nullified**, which stated that “the business activity register is open and personal data contained therein are not subject to the provisions of the Act of 29 August 1997 on the Protection of Personal Data”. This means that since **1 January 2012 the provisions of the Act on Personal Data Protection shall apply to the information identifying entrepreneurs in business trading**, if – in specific factual circumstances – they constitute personal data within the meaning of Art. 6 of the Act on Personal Data Protection. Thus the controllers of personal data relating to entrepreneurs will have to fulfil the obligations resulting from the Act on Personal Data Protection, including those concerning the registration of personal data filing systems.

2. Telecommunications law – Implementation of Directives 2009/136/EC and 2009/140/EC

The Ministry of Administration and Digitisation presented draft amendment to the Act of 16 July 2004 – Telecommunications Law, aimed among others at implementing the provisions of Directives 2009/136/EC and 2009/140/EC into the Polish legal order.

The draft includes provisions implementing into the Polish law Art. 4 para. 3 of the Directive 2002/58/EC on privacy and electronic communications regarding the obligation of data breach notifications and Art. 5 para. 3 of this Directive concerning the storage by website administrators of text files (so called cookies) in terminal equipment of web users.

As regards Art. 4 para. 3 of the Directive 2002/58/EC, the draft introduces the obligation to immediately (within 3 days from breach identification at the latest) notify the data protection authority of personal data about breaches, which may adversely affect personal data or privacy of a subscriber or an end user being a natural person. Whereby it was specified that personal data breach which may adversely affect personal data or privacy of a subscriber or an end user being a natural person shall mean such a breach which can in particular lead to his/her identity fraud or theft, significant material or personal damage, revealing banking secrecy or other professional secrecy protected by the act.

The draft introduces also the obligation for telecommunications operators to notify in particular circumstances of the breaches concerned the subjects whose data have been breached, whereby the information addressed to data subjects should contain hints on the activities which should be taken in order to limit possible results of a breach.

Regardless of the obligation to notify a data protection authority of personal data breaches, the draft amendment to the telecommunications law imposes on telecommunications operators also the obligation to notify the Office of Electronic Communications of network or services security or integrity breaches, which may disrupt data transfer, as well as of undertaken remedial actions.

As regards Art. 5 para. 3 of the Directive 2002/58/EC concerning placing and storing cookies, the draft provides for an „Opt-out” option, justifying it with the fact that a user can set in

browser's settings that cookies will not be stored on his/her device (equipment). The Inspector General for Personal Data Protection (GIODO) takes an opposite standpoint in the case concerned pointing at incompliance of the proposed solutions with the Directive above.

The draft amendment to the Telecommunications Law provides for shortening the retention data storage period from 24 to 12 months. However, the issue of accurate indication of circumstances and entities to whom the retention data can be disclosed still remains unresolved.

3. Public debate on direction of further changes in the Act on Personal Data Protection.

Mentioned at meeting in Canada and Berlin public discussion of the Inspector General for Personal Data Protection with academics on direction of further changes in the Act on Personal Data Protection has been also continued recently, including period after 25th January, when the European Commission published a new legal framework for European data protection. Wide discussion on the proposed new legal framework has been commenced by the **conference** which took place on 7th March 2012 entitled **"Reform of Personal Data Protection Rules in the European Union. Preliminary assessment of its scope and consequences"**. The organisers of the event were the Inspector General for Personal Data Protection, Poland's National School of Public Administration and the European Commission Representation in Poland.

4. Inspection activity - inspections in the sector of telecommunication operators.

In the second half of 2011 a number of inspections at telecommunication providers took place. The main aim was to check the fulfilment of obligation of deletion of traffic data after 24 months from their record (Art. 180 (1) of the Telecommunications Law). The results have shown that majority of the operators fulfils their obligation exactly after 24 months. In few cases a little bit longer storage periods by about 1 month have been noted, explained by the cyclicity of data deletion operations. Cases of longer retention than exact 24 months were noted mainly at small local operators.

5. e-Government - establishing of the Ministry of Administration and Digitisation.

In November 2011 regulation of the Council of Ministers establishing the Ministry of Administration and Digitisation composed of parts of the ministries, i.e. the Ministry of the Interior and Administration and the Ministry of Infrastructure, came into force. Tasks of the new ministry include among others:

- coordination of activities concerning implementation, functioning and modifications of Electronic Platform of Public Administration Services (ePUAP), Central Repository of Documents Patterns and Central Repository of Public Information.
- international cooperation as regards computerisation of public administration as well as information society, especially with relation to actions concerning coordination and monitoring of implementation of Digital Agenda for Europe.
- drafting changes in the Country Computerisation Plan
- monitoring of legislative activities concerning computerisation of public administration and development of electronic administration
- designing legal, organisational and technological bases for development of computerisation of public administration.
- coordination of undertakings concerning development of information society undertaken by institutions occupied by public tasks as well as supporting of non-governmental initiatives.
-

6. Conferences and events

On 9 December 2011 a **scientific conference entitled “Security of biometric technologies – biometric data protection”** was organised in Warsaw by the Faculty of Law and Administration of Cardinal Stefan Wyszyński University and the Inspector General for Personal Data Protection. The topics of the event included: biometrics and human rights, protection of biometric data and of their processing, use and securing of biometric identification in public administration, banking, IT companies and other public sector’s entities, as well as biometrics in work relations.

1. 6th Data Protection Day – 28 January 2012

On the occasion of the European Data Protection Day, which was celebrated in Poland for the sixth time, on 30 January 2012 the Inspector General traditionally organized an Open Day for all citizens at the seat of his Bureau. During the Open Day everyone had an opportunity to obtain legal advice as well as educational and informational materials. On the same they a conference under the slogan "What does the State know about its citizens? The principles of data processing in public registers" was held. Also, as usual the European Data Protection Day was celebrated in Brussels, where Dr Wojciech Rafał Wiewiórowski held a meeting with Members of the European Parliament (24 Jan.), he took active part in the 5th International Conference on Computers, Privacy and Data Protection (25 Jan.) and he organised the solemn meeting of the experts of data protection in the Republic of Polish Permanent Representation of the Republic of Poland to the European Union (24 Jan.).

Additional events related to the celebration of the Data Protection Day included:

- 27 January 2012, Gliwice – the game entitled “DATA served on a tray” designed for schools which participate in the project „Your data, your concern”. Educational initiative addressed to students and teachers. The Game, organized by the Gliwice Training Centre (Gliwicki Ośrodek Metodyczny) along with a branch of the Gliwice NGOs Centre “Active Youth Home” (Gliwickie Centrum Organizacji Pozarządowych „Dom Aktywnej Młodzieży”) consisted in finding and solving tasks concerning personal data protection. Students received maps according to which they will move between different checkpoints.

- 31 January 2012, Warsaw – chat with the Inspector General at the wp.pl portal. The subject of the conversation was what the State knows about its citizens, and on the other hand what the state should know about its citizens, and also what kind of information the State should not collect as well as not process.

7. Agreements on cooperation

On 8 December 2011 the Inspector General for Personal Data Protection concluded the Agreement on cooperation in the field of personal data protection and the right to privacy with the University of Lodz. The field of cooperation shall comprise scientific and research activity, education, publication, promotion and organisation related activity.

On 12 December 2011 the Inspector General for Personal Data Protection concluded the Agreement on terms and conditions of cooperation with the Supreme Audit Office. The cooperation between the two authorities shall relate to provision of collective information on results of conducted personal data protection audits, participation in courses and training organised by the parties, in informational meetings, mutual exchange of experience, conducting joint inspections on specific themes and consultations on the audits methodology.

PORTUGAL

Portuguese personal data protection most relevant legislation enacted in the period going from November 2011 to May 2012 (in Portuguese)

[Law n.º 5/2012 Of the 23rd January](#)

Regulating the processing of personal data using information technologies in order to build health national databases within the framework of the National Health Service.

[Law no. 9/2012 of the 23rd of February](#)

Third change to Law no. 1/2005 of the 10th of January regulating the use of video surveillance by the forces and security services in public places.

[Law no. 15/2012 of the 3rd of April](#)

Creates the National Death Certificate Information System (SICO)

[Law no. 17/2012 of the 27th of April](#)

Defines the legal framework applicable to the Community postal services within the framework of full market competition in the national territory as well as of international services from or to the national territory transposing to national law Directive no. 2208/6/EC of the European Parliament and of the Council of the 20 February 2008

[Resolution of the Assembly of Republic no. 63/2012 of the 4th of May](#)

Election of the Chair and of one commissioner of the Comissão Nacional de Proteção de Dados (National Commission for Data Protection)

SERBIA / SERBIE

1. Legal Framework

Since December 2011 there have not been changes to the Law on Personal Data Protection. The accompanying regulation is still lacking (e.g. a bylaw on measure of storing and security of sensitive personal data is still lacking – deadline was May 2009).

The Constitutional Court of Serbia passed decision on unconstitutionality of provisions pertaining to Military intelligence and securities agencies allowing access to retained data on e-communication without a court order. The Law was challenged by Commissioner for Information of Public Importance and Personal Data Protection and the Ombudsman together with the challenge of similar provisions in the Law on Electronic Communications, adopted in 2010. This case is still pending.

In December 2011 Commissioner submitted Ministry of justice with draft amendments to Law on Personal Data Protection pertaining to video surveillance. No feedback has been provided.

Regulatory framework on Data Protection is not fully in place. Collection of processing of personal data is envisaged in great number of bylaws pertaining to various fields, contrary to the constitutional provisions that data protection collection and processing is only allowed if prescribed by law adopted by National Assembly (and of course, based on consent).

2. Major Cases

Commissioner finalised the first **Systemic Supervision** of personal data protection within the Ministry of Interior and police forces in Serbia.

The number of cases is in constant increase. The Commissioner is currently conducting a supervision of the main e-communication service providers focusing on access to e-communication by state authorities, namely by intelligence service, prosecutors, police forces and courts.

3. Commissioner's Office

There have been no changes with regard to adequate resources of the Commissioner.

As mentioned in the previous report, "Commissioner still lacks adequate **premises**. This affects the process of the hiring of new **Staff members**. The **number of cases** pertaining to personal data protection is in constant increase, reaching even more than 100 cases per month of various natures – e.g. individual complaints, requests for interpretations of the Law, requests for opinion on compliance of actions/regulation with personal data protection."

Commissioner for Information of Public Importance and Personal Data Protection is competent for both personal data protection and freedom of information. The overall number of currently employed staff is 40 (39 + 1 contract), out of which 17 in the field of personal data protection.

4. Data Protection Day, 28 January 2012

The Commissioner hosted a one-day (Monday 30, January) with the Ombudsman and the Head of Council of Europe Office in Belgrade. During the working part of the event, the Commissioner presented significant data protection cases from 2011 and challenges of protection of personal data and privacy in Serbia.

On the day of 28 January, a self-evaluation test on personal data protection was published in one of the newspaper with the highest circulation in the country.

5. Projects

Capacity building of the Office of the Commissioner commenced in April 2012 as a Twinning Light Project, supported through the European Union funds (IPA 2009), implemented by the Information Commissioner of Slovenia. The project, in brief, envisaged improvement of data protection legislative framework, preparation of manuals, development of procedures and tools for Commissioner's staff as well as for main data controllers such as those in the field of internal affairs, health care, social affairs, electronic communications and other. The overall budget is €250.000.

Education of data controllers and CSOs representatives – Commissioner took part in a number of projects pertaining to awareness raising and capacity building. As an extension of a last year project, in late May 2012, the Commissioner will organised 4-day seminar for the representatives of 20 civil society organisations. The aim of the seminar is to acquaint CSOs' representatives on personal data protection challenges and to improve knowledge and develop skills to identify personal data protection issues and provide counsel to individuals. The aim is to build up expertise within CSO in order to make them more competent in personal data issues, and project, as well to ease the task of the Commissioner in performing its duties. This mainly with regard to education and awareness rising.

SLOVENIA / SLOVÉNIE

A. Position and competences of the Information Commissioner

The Information Commissioner of the Republic of Slovenia was established by the Information Commissioner Act² (hereinafter: the ICA) that merged two authorities, the previous Commissioner for Access to Public Information and the Inspectorate for Personal Data Protection within the Ministry of Justice. Thus, the Information Commissioner commenced operating on 1 January 2006 as an independent national supervisory authority performing its dual function as the “guardian of the right to know” and as the personal data protection authority. The Head of the Information Commissioner, who has the position of a state official, is appointed by the National Assembly for a 5 year term of office, renewable only once. In addition to adequate legal status, financed directly from the state budget (funding is allocated by the National Assembly on the proposal of the Information Commissioner) and staffed by the officials mandated with full inspection and offence competences, the Slovenian Information Commissioner is qualified to perform its function of data protection authority in entirely independent manner.

Among other competencies determined by the ICA, the Information Commissioner is the inspection and violations authority in the area of data protection in accordance with the Personal Data Protection Act³ (PDPA), performing also specific supervision functions under special legislation in the areas of patient rights, electronic communications, public media, personal identification and travel documents, and banking.

Of particular importance is the Information Commissioner's competence to lodge an application at the Constitutional Court of the Republic of Slovenia for a constitutional review of law, other regulations and general acts with regard to a procedure being conducted in relation to access to public information or the protection of personal data.

The Information Commissioner is also an independent supervisory authority for the regulation of personal data transfer in accordance with the Schengen Agreement being responsible for the supervision of the national data collection.

B. A summary of the activity

Information Commissioner supervision role

In 2011 the Commissioner initiated 682 (599 in 2010) cases regarding **suspected breaches** of the PDPA provisions, 246 (36%) in the public sector and 436 (64%) in the private sector. Compared with previous years (624 cases in 2009, 635 in 2008, 406 in 2007 and 231 in 2006) a dramatic increase in caseload ceased and has been stabilized during last 4 years. In both sectors the most common suspected breaches are of similar nature, involving unauthorised disclosure of personal data by transfer of data to third persons or by unlawful publication of data,

² Official Gazette of the RS, No. 113/2005.

³ Official Gazette of the RS, No. 94/2007

unlawful collection of data, inappropriate security of data, abuse of data for the purpose of direct marketing and unlawful video surveillance. Upon the examination of complaints received and due to *ex officio* procedures, 186 **inspection procedures** were initiated against public sector legal entities and 323 against legal entities in the private sector. In 2011 also 136 **offence procedures** were initiated, of which 43 against public sector legal entities, 66 against private sector legal entities, and 27 against individuals. Compared with the previous year the number of inspection procedures (150 in 2010) increased while the number of offence procedures (179 in 2010) decreased.

In addition to the inspection and offence activity the Commissioner performs other tasks as provided by the PDPA. The Commissioner issues **non-binding opinions and clarifications** on specific issues regarding data protection raised by the individuals, data controllers, public bodies and international bodies. In 2011 the Commissioner received 2143 requests (1859 in 2010) that, in addition to a significantly growing trend, are also becoming ever more demanding, which may be attributed to the transparent work and intensive public campaigning of the Commissioner. It is to be added that the Commissioner's staff answer daily to the phone calls related to data protection queries which amount to several thousand every year.

The Commissioner is under PDPA also competent to conduct **prior checks** regarding biometric measures (8 decisions in 2011), transfer of data to third countries (2 decisions in 2011) and connection of public filing systems (8 decisions). The data controllers in such cases need to firstly obtain the Commissioner's permission. Affirmative decisions concerning the implementation of **biometric measures** are granted to those legal entities where it is established that biometric measures are vital to the performance of activities, the safety of employees and property, as well as the protection of classified information or business secrets. Implementation of biometric measures was thus authorised in a case where access to telecommunications room, where servers containing business secrets and computer equipment of high value were located and needed to be protected. Implementation was also authorised in a case of access to the so called clean spaces in high-tech laboratories where processing and storage of genetic material takes place, in case of laboratories for validation of drugs, in case of objects where devices containing classified information are being destroyed, and in case of an area with an ion accelerator. Prior check is also needed in case of **linking of filing systems** that contain sensitive personal data or if the same connecting code is used for linking. In 2011 authorisation for linking was given to the Supreme Court of the Republic of Slovenia and to the Ministry of Interior in the case of the establishment of e-Land Register, and to the Central Population Register (CPR), general hospital and Ministry of Interior in the case of e-Birth application, where a link was made between general health records, CPR, and Civil register. The Ministry of Labour, Family and Social affairs was given permission to establish a link between the Central register of the public funds right holders and 15 other registers (e-Social services).

In 2011 the Commissioner received 85 appeals (equally in 2010) concerning the **right to access** one's personal data. However, a repeated increase was noted in the number of cases due to the non-responsiveness of personal data controllers (52% of appeals compared with 38% in 2010 and 51% in 2009), i.e. data controllers who do not respond in any manner to individuals' requests related to accessing their own personal data. Also significant increase has been noted

in the appeal procedures concerning access to medical records under the Patients Rights Act (18 appeals in 2011, 4 in 2010 and 8 in 2009).

Under the Constitutional Court Act the Information Commissioner is authorised to initiate the procedure for the **review of the constitutionality or legality** of regulations or general acts issued for the exercise of public authority, provided that a question of constitutionality or legality arises in connection with a procedure it is conducting. In 2011 the Commissioner requested a review of constitutionality of particular Real-Estate Recording Act provisions which because of their vagueness lead the Surveying and Mapping Authority to make certain personal data of the real estate owners registered in building and land cadastres public online. The Commissioner nevertheless holds that the world web should not be understood as appropriate “distribution environment” for the personal data in question, especially in the case of data base of such extent. Furthermore, the constitutionality and legality of the said provisions is questionable for the reason of the uncertainty of the purpose of these personal data processing.

Significant case law

The Commissioner has handled several interesting cases in its inspection procedures and developed rich case law. Below we present some of the cases interesting because of the number of breaches, the weight of the breach or content significance.

Collection of employees’ and candidates’ data

Privacy at workplace is a problematic area because of vague legal regulation and because of a large scope of offences. In the inspection procedures personnel files are being inspected in order to see what data are being processed by the employers. The employees’ personal data may only be processed if stipulated by law therefore employees’ consent is not regarded as adequate legal grounds, even though the employers tend to make this argument. Because of unequal power relationship consent in the employment relationship cannot be regarded as freely given. When the Commissioner finds that personal data has been processed without legal grounds (for example data in various questionnaires at the beginning of the employment relationship), the deletion of such data is ordered. According to the law, if the legal basis for processing of personal data ceases to exist, the data must immediately be erased and stop being used. This holds also in the cases of unlawful (often also unmarked) copies of personal documents retained by employers “for the purpose of verification of data accuracy”. A distinction also needs to be made between data of the candidates for an open position and employees’ data. In the case of candidates, only the data needed for assessment of candidate adequacy may be processed, excluding data such as personal identification number, tax number or bank account number that may only be processed in the case of employees.

Inadequate security of data in online forum

The Commissioner received a complaint about online matchmaking forum users’ names, e-mail addresses and passwords being disclosed online. It has been established that the operator of the website entrusted the design of the website to an Indian contractor, which did not act according to Slovenian legislation. The product did not include measures for traceability of the

data processing, and poor programming enabled the perpetrator to gain data on 7000 users of the site. The website operator was also found in breach of the provisions on contractual data processing, because it did not conclude a contract with the data processor. A data transfer to third countries without legal basis was additionally established. The Commissioner ordered the website operator to stop the processing of data and to notify all the users of the forum of the incident. The website operator decided not to establish the forum again, due to the high number of breaches.

Disclosure of personal data in sending e-mails

The Commissioner handled a number of cases where unlawful disclosure of e-mail addresses, regarded as personal data, took place. In all the cases the senders of the message did not put in place appropriate safeguards for data security – all the e-mail addresses were included in the field »To« or »Cc« and were thus disclosed to all the recipients of the e-mail. In one of the cases a notification to unsuccessful candidates for a position was sent by the data controller, who was not aware of the breach, because a dedicated application for handling documentary sources was used for sending the e-mails. The data controller apologised to the recipients and explained what had happened. It instructed its employees on the process of sending e-mails to multiple recipients.

Disclosure of personal data to applicants under the Access to Public Information Act (APIA)

The Commissioner handled a number of cases where public bodies, liable under the APIA, disclosed to the applicants the requested data, whereby also legally protected personal data were disclosed. It has been established that the liable bodies did not take appropriate measures to anonymize certain personal data, such as on the recipient of the document, on education, maiden name or even personal identification number of civil servants. When the requested document contains personal data protected by law, the body has to grant partial access, in the way that personal data in the document are not disclosed.

Publication of images where the individuals may be identified

The Commissioner handled a case where spatial photography containing images with identifiable individuals was published on the website of a professional photographer. The Commissioner stopped the procedure because the photographer removed all the images taken in Slovenia from the website on his own initiative. In the procedure spatial photography was considered in the context of the purpose of publication and identifiability of the individuals in the images. The Commissioner held that images taken and published in the course of reporting on a public event generally do not represent an issue, even if individuals can be identified. In this case the legal interest of the photographer for the publication of the images overrides the interest of the individual taking part in the public event. However the images of geographical locations, not reporting on an event, but containing images of identifiable individuals are problematic. The Commissioner held that the purpose of depiction of natural and cultural heritage could be achieved also without depiction of identifiable passers-by. The interest of the photographer in the publication in that case doesn't override the interest of the passer-by to decide freely whether he/she wishes to be identifiable in the image. That is why such images

have to be rendered anonymous before publication on the internet since the internet brings a new dimension to the publication of images and data protection. The images published on the internet may be accessed by anyone, more and more tools enable facial recognition and the images may be compiled into new filing systems. In its related opinion the Commissioner also pointed to the difference between street photography and spatial photography. The purpose of the latter is depiction of parts of urban areas or architecture, whereas the purpose of street photography is depiction of an individual in public places in special circumstances, situations and interactions.

General state of play of personal data protection in Slovenia

According to the Commissioner a significant increase in cases handled can be attributed to ever higher awareness of Slovenian citizens of their rights on data protection. The Commissioner also found that increasing tendencies on the surveillance of electronic communications are emerging. Such is the case of widening of the scope of competencies of law enforcement regarding the use of data, stored by the operators of the electronic communications (e. g. Data retention). The Government proposed amendments to the Criminal Procedures Act, by which the data on the whole mobile communications base station and not only on one specific phone number could have been acquired by the police. The Commissioner insisted that the approach is highly disproportionate and achieved the removal of the proposed amendment in the Parliament. This is a case that proves one more time that establishment of vast data bases leads to greater appetites for the data and function creep. It also shows lack of impact assessment before establishment of such filing systems, with great impact on privacy. In this context it is necessary to point also to great engagement of the Commissioner in informing the public on ACTA.

The increase of the direct marketing via e-mail was also noted, where the recipients are often not informed about their rights to cancel the use of their data for such purpose. The senders are often unable to explain how the e-mail addresses were gathered. As already mentioned, in this context also a number of cases where e-mail addresses were unduly disclosed, were handled by the Commissioner. In the area of video surveillance we also note an increase, especially in the areas where such surveillance is not lawfully permitted, e. g. in saunas, personnel rooms, lifts and certain public spaces, and for purposes not lawfully permitted such as employee surveillance. Most often the breaches include vague records of access to video surveillance footage and footage use, inadequate information on the implementation of video surveillance, etc. We often note inadequate security of personal data, collected online. In many cases data may be accessed with the use of search engines, where an entered personal name leads to data on e-mail address, user names, and passwords for user accounts on certain portals, or to the data on users that have ordered certain products online.

A number of data controllers are faced with the dilemma whether to use cloud computing services, for all the benefits they offer, such as accessibility, affordability, and flexibility. However cloud computing raises specific risks regarding information security and transfer of data to third countries and doubts regarding its compliance with data protection legislation. The Commissioner has issued and published a number of opinions on this subject and recently also special guidelines on cloud computing have been prepared.

C. Other activities of the Information Commissioner

The Commissioner continued its preventive work, privacy impact assessments in specific planned projects, and actively participated in a number of work groups. It is necessary here to mention the inter-departmental work group where the main focus was establishment of the safer and user friendly e-identities, and inter-departmental work group on the strategy of the information society development in the period between 2011 and 2015.

The Commissioner expanded the scope of its tools for **awareness raising** in the 2011. Along with constant communication with the media, a great number of opinions, guidelines and brochures, published on the website www.ip-rs.si, the Commissioner introduced a new format of special reports that aim to shed light on specific areas that need to be uncovered in terms of data protection practices. The first of the reports covered loyalty cards, an ever more used tool for gathering data on consumers, for segmentation and targeted marketing. The findings were published by a number of media.

Each year the Commissioner also organizes an event on the European Data Protection Day and the World Right to Know Day, on the September 28. The report on the former is dealt with separately. On the occasion of The Safer Internet Day (February 7) the Commissioner joined forces with the Centre for safer internet SAFE.si in public campaigning on this year's theme about connecting generations under the slogan: "Discover the digital world together... safely!"

The Commissioner takes an active role in **preparation of legal acts and other legal documents** by giving an opinion as to the compliance with the provisions on personal data processing, as stipulated by the PDPA. In 2011 the Commissioner advised in preparation of the legislation that governs data processing in health system, underage delinquents, real estate records, road tolling, records of places of residence, electronic commerce and electronic signature, higher education, children with special needs, parliamentary election, tax procedure, criminal procedure, penal code, etc. The Commissioner has also followed closely the development of the new EU Draft Regulation on the protection of personal data and presented its comments and suggestions to the Commission as well as to the Working Party 29.

In terms of **international cooperation** the Information Commissioner as the national data protection authority, cooperates with competent bodies from other EU Member States and the Council of Europe, namely in the Article 29 Working Party, in the Joint supervisory body for Europol (where the Information Commissioner is in the role of the vice president), Schengen and Customs, and in the T-PD under Convention 108. The Commissioner is also active in the International Working Group on Data Protection in Telecommunications and in the Working Party on Police and Justice.

The rich international activity is complemented with attendance at international meetings, such as the International Conference of Data Protection and Privacy Commissioners and International Conference of the Information Commissioners. The latter has given a mandate in Ottawa to the Slovenian Information Commissioner to establish a website of all the Information Commissioners, that was presented to the public in November. Experts of the Information Commissioner have actively participated in a number of international seminars and workshops.

The Information Commissioner participates as a Junior Partner in a twinning project »Implementation of Personal Data Protection Strategy« in Monte Negro. At its seat it hosted representatives from similar authorities from Croatia, Serbia, Kosovo, Monte Negro and Macedonia.

The activities of the Commissioner are widely publicized. Therefore it is not surprising that in national public opinion research (Politbarometer) the Information Commissioner ranks first among the state bodies and public institutions that citizens trust the most.

SWITZERLAND / SUISSE

Évaluation de la loi sur la protection des données

Une évaluation de la loi fédérale sur la protection des données a été effectuée sur mandat de l'Office fédéral de la justice. L'évaluation montre que d'une manière générale la LPD permet en soi d'atteindre les objectifs visés. Elle débouche cependant sur un constat selon lequel les menaces qui pèsent sur le respect des droits et des libertés fondamentales lors du traitement de données personnelles se sont renforcées ces dernières années. Les individus ont toujours plus de peine à conserver la maîtrise sur les données qui les concernent. L'évolution technologique et le volume de données qu'elle engendre sont des défis considérables non seulement pour les individus, mais aussi pour les responsables de traitement et les autorités de protection des données. Ainsi les évaluateurs reconnaissent que si le préposé fédéral remplit son mandat légal avec un haut degré d'efficacité, il rencontre néanmoins « des difficultés croissantes à exercer son mandat de surveillance étant donné l'accroissement constant de la fréquence, de l'opacité et de l'internationalisation des traitements. ». Ils relèvent un déficit au niveau de l'exercice des droits des personnes concernées. Ce déficit découle notamment du fait du coût et de la longueur des procédures. Il provient également du fait de l'importance et l'ampleur des données collectées quotidiennement et du fait que trop souvent les personnes ne prennent pas suffisamment conscience que des données sont collectées et traitées à leur égard. Le Conseil fédéral dans un rapport qu'il a adressé au Parlement convient que la loi sur la protection des données doit être adaptée « aux rapides développements technologiques et sociétaux intervenus depuis son entrée en vigueur » et « prendre en compte les nouvelles menaces. » Il a donné mandat au Département fédéral de justice et police de faire des propositions d'ici 2014.

Ce travail de mise à jour et de révision de notre droit de la protection des données devra tenir compte des travaux en cours au sein de l'Union européenne en vue d'un nouveau cadre juridique de protection des données et au Conseil de l'Europe avec la révision de la Convention 108. Le Conseil fédéral souhaite également examiner la répartition des compétences entre la Confédération et les cantons en matière de législation et de mise en oeuvre, ainsi que l'introduction de mesures d'autoréglementation et un renforcement éventuel de l'indépendance du Préposé fédéral à la protection des données et à la transparence.

Modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure

Dans le cadre de la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, le régime du droit d'accès des personnes concernées a été modifié. Dès le 1^{er} juillet 2012, les personnes concernées bénéficieront d'un droit d'accès direct et s'adresseront directement au service de renseignement de la Confédération pour faire valoir leur droit. L'accès pourra cependant être différé dans trois cas :

- Les données traitées concernant le requérant sont liées à des intérêts prépondérants qui exigent le maintien du secret dans le cadre de la détention précoce et de la lutte contre les dangers en matière de terrorisme, de service de renseignement prohibé, d'extrémisme violent, des actes préparatoires relatifs au commerce illicite d'armes et de substances radioactives et du transfert illégal de technologie ainsi que dans le cadre d'une poursuite pénale ou d'une autre procédure d'instruction.
- Les intérêts prépondérants d'un tiers l'exigent

- Aucune donnée concernant le requérant n'est traitée.

En cas de refus ou de report de la demande de renseignement, le requérant en est informé et a la possibilité de demander au Préposé fédéral à la protection des données et à la transparence de vérifier le traitement. Le préposé peut en cas d'erreur adresser une recommandation au service concerné. Il informe le requérant qu'aucune donnée le concernant n'est traitée illégalement ou qu'en cas d'erreur relative au traitement ou au report de la réponse, une recommandation a été adressée au service concerné. Suite au contrôle du préposé, le requérant peut s'adresser au Tribunal administratif fédéral. En cas d'erreur, le Tribunal adresse au service concerné une décision lui ordonnant d'y remédier. Le service concerné communique au requérant les renseignements qu'il a demandés dès que les intérêts liés au maintien du secret ne peuvent plus être invoqués, mais au plus tard après l'expiration du délai de conservation. Le requérant qui n'est pas enregistré en est informé au plus tard trois ans après réception de sa demande. Le préposé peut exceptionnellement recommander de fournir immédiatement le renseignement demandé lorsque cela ne menace pas la sûreté intérieure ou extérieure.

Outil de sensibilisation à la protection des données et à la transparence (Thinkdata.ch)

A l'occasion de la 6^e journée de la protection des données, le 28 janvier 2012, un outil de sensibilisation à la protection des données et à la transparence (Thinkdata.ch) a été présenté et mis en ligne (version en français actuellement). Cet outil interactif s'adresse aux administrations et aux entreprises, ainsi qu'aux utilisateurs et aux personnes concernées par les traitements de ces organisations, en fonction de leur métier ou de leur rôle dans l'organisation (cadres, responsables des ressources humaines, responsables IT, employés, ...). L'outil présente sous l'angle des métiers mais également des types de données différents scénarios inspirés d'histoires réelles. Ces scénarios relatent un problème lié à la protection des données ou à la transparence dans le but de sensibiliser l'utilisateur de l'outil. Des conseils sont associés aux scénarios pour permettre aux utilisateurs de se positionner et d'améliorer le traitement des données au sein de leurs organisations

Suite aux réactions positives reçues depuis la mise en ligne de ce service, une deuxième version est en préparation. Elle devrait en particulier être multilingue (notamment allemand et anglais) et si possible déborder le cadre purement helvétique.

Le service est accessible sous www.thinkdata.ch

Rapport d'activité

Le Préposé fédéral à la protection des données et à la transparence présentera son 19^e rapport d'activités lors de sa conférence de presse annuelle, le 25 juin prochain. Le rapport pourra être consulté sur www.edoeb.admin.ch

THE FORMER YUGOSLAV REPUBLIC MACEDONIA / L'EX-REPUBLIQUE YUGOSLAVE DE MACEDOINE

28th January, 2012 Celebration of Data Protection Day

On the occasion of the European Data Protection Day, 28 January, the Directorate for personal data protection of the Republic of Macedonia, Project – Support to the Directorate for Personal Data Protection and Microsoft Macedonia organized celebration under the motto “**Click safe**”.

Common goal of the Directorate, the Project – Support to the Directorate for Personal Data Protection and Microsoft Macedonia was to increase the public awareness for the children's safety on the internet and in the same time increasing the awareness of the teachers and parents about children's activities on internet.

In order to popularize the event, the Directorate and Microsoft Macedonia announced poetry and art competition “Click Safe” for the children from primary schools across the country in December 2010. The selection of the best 15 poems and 15 drawings was made and all of them were put on an exhibition during the event organized on 27 January.

The event was divided in two parts, conference where the actual open questions regarding the safe use of internet were discussed by the Ministry of Education, the Directorate, the Ministry of Interior, Microsoft Macedonia and the representatives of the schools. During the conference, awarded children were divided into 5 groups, in separate hall creating videos, songs and other creative projects which were presented at the end of the conference.

The event was covered by most of the media.

15 March – Day of Consumers – Mu number – my protected world

On the occasion of the marking of the Day of Consumers, 15 March, and in order to raise the public awareness of the protection of the personal data of the consumers in the telecommunications sector, the Directorate for Personal Data Protection, the Agency for Electronic Communications, the Consumers' Organisation of Macedonia, T-Mobile Macedonia, VIP OPERATOR, ONE Telecommunications Services, Makedonski Telekom and Alo Telekom have signed Declaration on cooperation for joint organization of Open Days - Protection of the Personal Data of the Consumers under the motto MY NUMBER - my PROTECTED WORLD!

The purpose of this joint project was to create conditions for the application of the contemporary developments in terms of the processing of the personal data through the information technology in the everyday operation of the operators of public electronic communication services and for better protection of the consumers, as well as to raise the social responsibility of the business operators towards the consumers and the community.

SIN - Software for inspection implemented

This software solution was installed in the reporting period and all the preconditions for electronic performance of the inspection were met. This software, through internet can be used out of the premises of the Directorate, will contribute to more efficient and economic

performance of the inspection procedure, generating reports and planning inspections. The inspection procedure is completely realized on the spot during the course of the inspection which contributes in cutting of post expenditures and the time needed for the procedure and in raising the efficiency of the inspectors. Namely, the software is designed in accordance to the specific needs of the inspectors from the Directorate in a way that allows generating minutes from the inspection in a form of a check list. The task of the inspector is to answer the questions and print it out.

Cooperation with media

Directorate for personal data protection continued with direct cooperation with two media, the daily newspaper New Macedonia and the Macedonian Radio Television, through which the citizens are informed on a weekly basis about protecting of their right of privacy.

Through the web portal of the newspaper New Macedonia, citizens have a possibility to ask questions regarding Data Protection. The Directorate meets them and prepared the answers that are published every Monday in the newspaper. Since the beginning of this cooperation, in June 2011 until the end of April 2012 there were published 41 articles in the daily newspaper.

Cooperation with the Macedonian Radio Television is in the form of regular participation of the staff from the Directorate in the morning program “Good Morning Macedonia”, where every Tuesday the current topic from protection of personal data is elaborate. Citizens have the opportunity of directly asking the questions in this open program. Starting from 2011, till the end April 2012, 34 discussions on different topics related with protection of personal data in this on line program were opened.

Besides the cooperation with these two media, the Directorate regularly meets all current issues that are in the focus of public interest and media.

IPA 2008, Component 1, Project – Support do Directorate for Personal Data Protection

DPDP is a beneficiary of IPA Instrument for pre accession assistance of the European Union, Program 2008 –Component 1, Project – “Support to the Directorate for Personal Data Protection”. The project have a goal to contribute in strengthening of the competences of DPDP, improvement of the implementation of legislation in the area of personal data as well as to raise public awareness of the citizens for their right of personal data protection. The project is consisted of four components: Alignment of domestic legislation with EU legislation; Strengthening institutional capacities of DPDP; Raising public awareness for the right of personal data protection as human right.

With support of the above mention project, the Directorate adopted a lot of bylaws regarding data protection in several fields, as follows:

1. Guidelines regarding the processing of personal data by means of smart cards and rfid tags
2. Guidelines regarding the introduction of biometric data

3. Guidelines on privacy by design and privacy impact assessment
4. Guidelines for video surveillance
5. Guidelines on personal data protection in social sector
6. Guidelines on personal data protection in employment sector
7. Guidelines on personal data protection in the health sector
8. Guidelines on personal data protection in insurance sector
9. Guidelines for education providers
10. Guideline for processing of personal data in the electronic communications sector
11. Guideline for processing of personal data in the banking sector
12. Guideline for processing of personal data in the police sector
13. Guidelines for the use of personal data in direct marketing
14. Analysis for direct marketing
15. Analysis for education sector
16. Analysis for healthcare sector
17. Analysis for insurance sector
18. Analysis for telecommunication sector
19. Analysis for employment sector
20. Analysis for social protection sector
21. Analysis for banking sector
22. Analysis for regulation on law enforcement sector

30 – 31 May 2012 - International Conference “Modernization of Data Protection Legislation in Europe”

Directorate for personal data protection will organize second international event in the Republic of Macedonia in the field of personal data - Conference for Modernization of Data Protection Legislation in Europe.

The conference will be realized with support from the Delegation of the European Union and the project team of IPA 2008 project "Support to the Directorate for Personal Data Protection" which was implemented in the period from January 2011 till June 2012.

In the frame of the conference, the novelties from the legislation for data protection will be discussed, as new EU Legislation and the principle of accountability, new role of the Data Protection Board, Modernization of the Convention 108, new EU legislation and the principle of data protection impact assessment, new challenges in cooperation between countries.

In the same time, the Directorate for Personal Data Protection is continuing with realization of its responsibilities regarding the inspection supervision, education, trainings and preventive roll for protection of the personal data in Republic of Macedonia.

UKRAINE

At the end of 2011 Ukraine concentrated its efforts on preparing by-law legislation on personal data protection. On the 30th of December the Order of the Ministry of Justice “The Model Procedure of Processing Personal Data in Personal Data Bases” was signed. The Model Procedure determines organizational and technical measures that ensure adequate protection of personal data by the controller.

For the second time in its history Ukraine celebrated on the 28th of January the Personal Data Protection Day. Media campaign aimed at increasing awareness of society was held during those days.

But the most significant event was presentation of analysis of the Law of Ukraine “On Personal Data Protection” on February, 13. The analysis was made by CE and EC experts within the Joint Program of the Council of Europe and European Commission “Promotion of European Media Standards in the Ukrainian Media Environment”. Within the project a couple of expert seminars were held and meetings of representatives of Ukrainian authorities, members of parliament and NGO’s were conducted.

Now the Ministry of Justice is finalizing drafting the Law on Amendments to the Law on Personal Data Protection. The Amendments aim to fulfill all international requirements on the protection of personal data. It is planned to present the draft law to the government by the end of April 2012.

UNITED KINGDOM / ROYAUME UNI

European Data Protection: Coming of Age

Ministry of Justice Minister Crispin Blunt spoke at the Council of Europe afternoon session at the Computer, Privacy and Data Protection [CPDP] conference entitled *European Data Protection: Coming of Age* in Brussels on Friday 27 January, the day before Data Protection Day. The Council of Europe session was called “European Privacy and Data Protection” and formed part of a busy programme during the UK Chairmanship of the Committee of Ministers. Crispin Blunt congratulated the Council of Europe on setting the benchmark for universal data protection standards, starting with the inception of Convention 108 in 1981, becoming the first and only binding international legal instrument with a worldwide scope of application in the field of data protection. However, changes in the modern world, in particular cloud computing, social networking and other forms of new technology, mean that this legal instrument must be adjusted to keep up with the times, alongside new data protection legal instruments being proposed by the European Union. He expressed the hope that by working together members can secure protections for the public without sacrificing the vital freedoms on which we all depend

Data Protection Day: 28 January 2012

In celebration of Data Protection Day, Lord McNally, Justice Minister with responsibility for data protection policy, published an article on the Justice website entitled “Protecting Our Data in the 21st century”. In it he explains why protecting people's data without sacrificing their freedom should be at the heart of privacy and personal data protection policy in 21st century Europe. He points out that this is a key time in the development of data protection legislation across Europe and in the wider international context, with the Council of Europe modernisation programme on Convention 108, and the publication of Data Protection proposals by the European Commission. On the occasion of Data Protection Day it was worth recognising the considerable achievement made by the Council of Europe in setting the benchmark for universal data protection standards. The inception of Convention 108 marked the formulation and agreement to a number of core principles which have governed the protection of up to 800 million individuals across 43 signatory countries with regard to automatic processing of personal data, and in doing so reconciling the free flow of information with privacy and data protection concerns. However, the extraordinary pace of technological innovation, increasing global interdependence and the growing transfer of people and information within and across borders presents a significant and unprecedented challenge. No one can be sure what further changes may be around the corner, but in a digital age of cloud computing, social networking and other forms of new technology we must be proactive in taking the right steps now to create an environment in which: business and enterprise can prosper; the police and judicial authorities are able to protect and serve the public effectively; and where individuals can be confident that their privacy, safety and freedom will be safeguarded.

Lord McNally's speech to a Westminster eForum seminar entitled: Data Protection and ePrivacy 2012: Responses to the European Data Protection Review

On Thursday 8 March 2012 Lord McNally spoke at the Westminster eForum seminar and took questions and comments from the audience alongside Peter Hustinx, European Data Protection Supervisor and David Smith, the UK's Deputy Information Commissioner. In his speech, Lord

McNally recognised the need for updated and harmonised legislation in light of technological changes and globalisation but also referred to the continued relevance of existing data protection principles and the need to reject a 'one size fits all' approach. He mentioned some of the Government's concerns about the EU's proposed Regulation, in particular, likely impacts of its more prescriptive requirements on organisations. However, he also pointed out that the Government was still considering the provisions in detail, and was continuing to consider views both within Government and externally, in particular via responses to the targeted Call for Evidence which was launched by the MoJ on 7 February and closed on 6 March (two days before the Seminar).

House of Commons debate on the proposed new EU Directive

A Parliamentary debate on the Directive took place on Tuesday 24 April. The debate focused on both the substance of the Directive and its legal base and the associated option of the UK exercising a Schengen opt-out under Protocol 19 of The Treaty on the Functioning of the European Union. The motion was not to exercise the opt-out under the Schengen Protocol, and instead rely on the limiting effect of Article 6a of the Opt-in Protocol, supplemented by more explicit recitals or amendments to the body of the Directive, to clarify its application to the UK. The result of the vote found in favour of not exercising the Schengen opt-out.

IAPP Data Protection Intensive

The International Association of Privacy Professionals held a Data Protection Intensive conference on 26-27 April, at which John Bowman, Head of the MoJ EU and International Data Protection Policy team spoke on the proposed new EU legal instruments, alongside Rosemary Jay, senior attorney from Hunton and Williams and Fedelma Good, Head of Marketing Privacy & Information Management, Barclays. Will Wormell, another member of the EU and International Data Protection Policy team, also spoke, alongside lawyer Eduardo Ustaran, Head of Privacy and Information Law, Field Fisher Waterhouse; Justin Weiss, Senior Director for International Privacy and Policy, Yahoo!; and Emma Butler, Senior Policy Officer from the Information Commissioner's Office, on the topic of "The Proposed New Law: Practical Implications for Internet Businesses".