Strasbourg, 2 October / octobre 2013

T-PD(2013)03Mos

CONSULTATIVE COMMITTE 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

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

TABLE OF CONTENTS / TABLE DES MATIERES

ALBANIA / ALBANIE 3

ANDORRA / ANDORRE 14

AUSTRIA / AUTRICHE 15

BELGIUM / BELGIQUE 16

CYPRUS / CHYPRE 18

CZECH REPUBLIC / REPUBLIQUE TCHEQUE 19

ESTONIA / ESTONIE 22

FINLAND / FINLANDE 23

FRANCE 25

GERMANY / ALLEMAGNE 26

GREECE / GRECE 30

HUNGARY / HONGRIE 31

IRELAND / IRLANDE 34

ITALY / ITALIE 35

LATVIA / LETTONIE 37

LIECHTENSTEIN 41

LITHUANIA / LITUANIE 42

MONACO 45

NORWAY / NORVÈGE 46

PORTUGAL 47

ROMANIA / ROUMANIE 48

SERBIA / SERBIE 50

SLOVAK REPUBLIC / REPUBLIQUE SLOVAQE 51

THE FORMER YUGOSLAV REPUBLIC MACEDONIA / L'EX-REPUBLIQUE YOUGOSLAVE DE MACEDOINE 53

UNITED KINGDOM / ROYAUME UNI 58

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”:

- **Has drafted and approved Instruction No. 18, dated 03.07.2012 “On processing of personal data in the framework of clinical testing of drugs ".**

This Instruction regulates some rights and obligations related to personal data protection and processing in the context of clinical trials of drugs in human beings, providing informed consent in which clearly defined purpose and recipient processing of personal data, personal data are processed and the time period for which consent is given, making anonymous personal data etc.

- **Has drafted and approved Instruction No. 19, dated 03.08.2012 “On regulating the relationship between controllers and processors in cases of outsourcing of data processing and usage of a template contract in cases of outsourcing ".**

The purpose of this instruction is to establish the rules regarding the relationship between controllers and processors in case of delegation of personal data processing, and adoption of a standard contract sample that the parties shall use for such delegation.

- **Has is drafted and approved Instruction on No. 20, dated 03.08.2012 “On Processing of Personal Data in the Banking Sector”.**

The purpose of this Instruction is to establish the rights and obligations of the banks, branches of foreign banks and financial non-bank entities in the framework of processing personal data in their banking activity.

- **Has drafted and approved Instruction No. 21, dated 24.09.2012 “On determining the rules for safeguarding personal data processed by large controllers”.**

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". The purpose of this Instruction is defining the technical and organisational measures for protection of personal data processed by large controllers, or processors, referred to as the subjects processing personal data, and the rules of their cooperation with the Commissioner.

- **Has drafted and approved Instruction No. 22, dated 24.09.2012 “On determining the rules for safeguarding personal data processed by small controllers”.**

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". In this instruction are treated the technical and organisational measures for protection of personal data processed by small controllers, or processors. Are provided the minimal standards for the security of personal data, this in line with measure of data processing.

- **Has drafted and approved Instruction No. 23, dated 20.11.2012 “On processing of personal data in health sector ".**

The scope of this Instruction covers organisations and natural persons operating in the health care system, as well as other bodies responsible for supervising, or controlling health care, and the data processors acting on their behalf.

- **Has drafted and approved Instruction No. 24, dated 26.12.2012 "On obligations of controllers prior to processing personal data".**

This Instruction abrogates the Instruction No. 2, dated 25.02.2010 "Obligations of data controllers and data processors prior to processing personal data". It aims at reformulating the previous obligations of controllers and processors in accordance with amendments to the law on protection of personal data and sublegal acts.

- **Approved the amendments of the Law no. 9887, dated 10.03.2008 "On protection of personal data" in 2012 is reflected in the respective changes in:**

  - Instruction No. 25, date 27.12.2012 "On same additions and amendments to Instruction No. 10, date 06/09/2011 "On processing of personal data in the context of hotel services".

  - Instruction No.26, date 27.12.2012 ""On same additions and amendments to Instruction No.4, date 16/03/2010 "On safeguard measures for personal data in the field of education"".

  - Instruction No.27, date 27.12.2012 ""On same additions and amendments to Instruction No.7, date 09/06/2010 "On processing of personal data in education sector"";

  - Instruction No.28,date 27.12.2012 ""On same additions and amendments to Instruction No.11, date 08/09/2011 "On processing of personal data in private sector"";

  - Instruction No.29, date 27.12.2012 ""On same additions and amendments to Instruction No.16, date 26/12/2011 "On protection of personal data in direct marketing and safeguard measures"";

  - Instruction No.30, date 27.12.2012 ""On one amendment to Instruction No.19, date 03/08/2012 "On regulating the relationship between controllers and processors in cases of outsourcing of data processing and usage of a template contract in cases of ousourcing"".

  - Instruction No.31, date 27.12.2012 "On specification of the terms and conditions for the exemption from relevant obligations for the processing of data for journalistic, literary or artistic purposes defining the criteria".

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". This Instruction sets out the basic terms on which the processing of personal data may be exempted from the obligations contained in Articles 5, 6, 7, 8, 18, and 21 of the Law, in order to reconcile individuals' right to the protection of their personal data with the rules governing the right to freedom of expression.

  - Instruction No.32, date 27.12.2012, "On same additions and amendments to Instruction No. 9, date 15.09.2010 "On the fundamental rules for the protection of personal data in written, audio and audiovisual media";

  - Instruction No.33, date 21.01.2013, ""On same additions and amendments to Instruction No. 21, date 24.09.2012 "On determining the rules for safeguarding personal data processed by large controllers";

- Instruction No.34, date 21.01.2013, ""On same additions and amendments to Instruction No. 22, date 24.09.2012, "On determining the rules for safeguarding personal data processed by small controllers"".

- **Has drafted and approved Instruction No. 35, dated 07.05.2013 "For the processing of personal data for the purposes of election campaign".**

This Instruction aims to define the rules for processing personal data of the candidates during the election campaign. Instruction brings several important innovations such as the provision of the obligation for the candidate to notify the Commissioner for the protection of personal data if he or a third party on behalf of its processes personal information for the purposes of the election campaign. Another innovation is the case provided that the candidate uses personal data processed for the purposes of direct marketing, such as. When the candidate contact with voters through phone messages, e-mail, mail, should first have the consent of the electorate.

- **Has drafted and approved Decision No. 3, date 20.11.2012 "On defining the states with adequate level of protection for personal data" and Annex 1 attached, which provides states with adequate level according to categories defined in the Decision.**

The Act recognizes controllers with public and private countries in which can transfer (Appendix 1) data without authorization request to the Commissioner. The decision constantly updated whenever ratify Convention 108 states have adopted the law on protection of personal data, have set up independent authorities for the protection of individual privacy, etc.. Updates are published on our official website of authority.

- **Has drafted and approved Decision No. 4, date 27.12.2012** "On defining the exemption cases from the duty to notify processed personal data".

This decision is prepared by the Commissioner for personal data protection in the framework of application and implementation of point 4 of Article 21 of Law no. 9887, dated 10.03.2008 "On Protection of Personal Data", as amended.

- **Has drafted and approved Decision No. 5, date 27.12.2012 "On some additions and amendments to Decision No.2, date 10.3.2010 "On defining the procedures for the administration, registration of data, data entry, processing and retrieval"".**

This decision aims redefining of the duties of controllers and processors in accordance with amendments to the Law on protection of personal data and sublegal acts but with practice in the field of personal data protection.

- **It has approved the Manual on Internal and External Communication of 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".**

- **Has drafted and approved the "Manual of Personal Data Protection in the Media".**

- **Has drafted and approved" Data sharing code of practice";**

- **Has drafted and approved "The Code on Use of Video-Surveillance Systems (CCTV)."**

- **Has drafted and approved the questionnaire on "International personal data transfer" was prepared, which is mandatory to be filled by any public or private controller.**

- **Has prepared Guidelines "Protection of personal data to companies Call Centre".**

- **The authority of Commissioner for personal data protection with the support of the expert of the project EU-IPA 2009, Mr. Emilio Aced Felez has drafted the "Practical Guide on Data Protection for Prosecutors";**

- **On July 2012 was signed the cooperation agreement between the Commissioner for Personal Data Protection and the Commissioner for Protection from Discrimination.**

This agreement will contribute to mutual cooperation and laid the foundation for ensuring the protection of personal data being alternately with the other fundamental human right such as that of protection from discrimination.

- **On December 2012 was signed the cooperation agreement between the Commissioner for Personal Data Protection and National Chamber of Notaries.**

The Parties hereby cooperation agreement aimed to establish a mutual cooperation between them in accordance with their respective legislations and international standard setting related to respect and guarantee the protection of privacy.

- **On January 2013 was signed the cooperation agreement between the Commissioner for Personal Data Protection and Tirana University Rectorate.**

The agreement aims to establish close relationships on implementation of the law in the protection of personal data in the University sector.

- **On May 2013 2013 was signed the cooperation agreement between the Commissioner for Personal Data Protection and National Chamber of Private Enforcement Agents.**

This Agreement is intended to expand the cooperation between the two institutions to contribute constructively in the process of implementing their respective legislation and enforcement by the National Chamber of Private Enforcement Agents the fines imposed by the Commissioner for Personal Data Protection to public and private controllers.

According to the Law "On personal data protection"- amended, advices and opinion have been given on draft legal acts and regulation in the field of data protection, as well as legal counseling for acts coming from the Council of Ministers, Ministry of Justice, National Council of Radio and Television, Central Inspectorate, Ministry of Interior, etc. and some private entities. As the most important among them would be:

- Has given a legal opinion on two draft laws coming from the Ministry of Justice. More specifically to:

- Draft Law "On the Right to Information" and
- Draft Law "On amendments to Law no. 9887, dated 10.03.2008 "On the Protection of Personal Data" as amended.

In the draft law "On the Right of Information", comments consisted only in correcting some references, while the draft law "On some amendments to Law no. 9887, dated 10.03.2008 " On personal data protection " as amended, is proposed addition of a new chapter titled "The person in charge of data protection."

- Has given a legal opinion on Draft Decision "On the criteria and documentation for entering, residing and treating the foreigners in the Republic of Albania" sent by the Ministry of Interior.

- Has given a legal opinion on Draft Law “On Asylum”, sent by the Ministry of Interior.

- Has given a legal opinion on “Drafting of Report concerning the Convention on Enforced Disappearances” and linking this Convention to the protection of personal data and the practices of the Commissioner in this regard.

- Has given a legal opinion on Draft Regulation “On protection, processing, preserving and securing of personal data”, prepared by the Albanian Agency for Development of Investments”.

- Has given a legal opinion on “Regulation on standardization of projects development in public administration” sent by the National Agency of Information Society.

- **Complaint Handling and Inspections**

Pursuant to the Law "On Protection of Personal Data", and the acts adopted by the Commissioner, for the period June 2012 - June 2013, the Department of Investigation-Inspection has conducted, in summary, as follows:

1. Complaints

- ✓ Over 64 Complaints;
- ✓ Regarding the the anonymisation of the data from controllers whom belong to the Media field;
- ✓ Regarding the anonymisation of the complaining entity data, in the publication of the courts decisions;
- ✓ Regarding the abuse of data through direct marketing;
- ✓ Regarding the monitoring of presence at work of employees in public institutions, through biometric transducer of finger sign;
- ✓ Regarding the ilegal transmision of personal data in third-party, by the banking institutions;
- ✓ Regarding the publication of false data to the media on subjects who were acquitted by a court decision;
- ✓ Regarding the SMS sent during the general election campaign.

2. Administrative Audit and Inspections-Recommendations, for these topics:

- ✓ About 147;
- ✓ Online publication of judicial decisions without anonymisation of the personal data and security measures for the system used by the courts;
- ✓ Drafting of internal regulations on the security of personal data processed and confidentiality;
- ✓ Setting the information table to inform the personal data subjects for the use of "observation-recording cameras" system and Respect of the Timeliness for the storage of records;
- ✓ Respect the right for access, of the data subject;
- ✓ Compliance with the duty to inform the data subjects;
- ✓ Processing of personal data by the usage of CCTV in public places by the General Directorate of State Police;

- ✓ International transfer of personal data collected by the public or private controllers;
- ✓ Data collection and processing of sensitive health data of vulnerable groups of data subjects, especially in preschool education.

3. Fines

- ✓ 12 Fines to Data Controllers.

4. Recommendations of the Commissioner

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);
- ✓ 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.

- ➢ **Drafting and Approval of the Commissioner's Acts**

In the context of the changes within the law no. 9887, date 10.03.2008 "On protection of personal data", during December 2012 the Registration Department has been working on the approval of some additions and amendments to the Notification Form and also to the Guide on how to complete the Notification Form from the controller. These changes were approved by the Commissioner's internal decision.

- ➢ **Sensibilization and awareness of personal data subjects**

During the period June 2012 - June 2013, among other priorities of the Registration Department's work has been the sensibilization of the controllers, the acquaintance with the Law no. 9887, date 10.03.2008 "On the Protection of Personal Data", and the implementation of their legal obligation to notify the Office of the Commissioner about the state of conditions of personal data processing.

In this context, the Registration Department has organized several awareness seminars with the Education Departments of Vlora, Fier, Elbasan, Kukes, Saranda, Gjirokastra, Përmet Lezha, and Durres as well as with the Education Department of Tirana District. Moreover in collaboration with the Prefecture of Tirana County, a set of workshops took place with Local Representatives of Tirana, where participants were introduced to the Law and the Commissioner's authority, relevance and innovation that this law brings and the central topic that was discussed extensively was the obligation that controllers have to notify the KMDP.

The final and very important product of these seminars has been the notification form, for which subjects were trained and assisted on how to fill it in the best way possible, in order to provide information required by this legal obligation. The participation in these seminars has been very large and it brought a considerable flow of notifications but also raised awareness on a wide geographical distribution. Furthermore, given the constructive conversations that took place in different moments of the seminar, various issues or complaints raised by these subjects, once as representatives of the controllers but mostly like personal data subjects themselves, were conducted to the proper department of the Commissioner's Authority, according to the case or nature of problem.

- **Management of notices and the public Register of controllers entities**

The KMDP office has been receiving a whole information system of notifications, requests for additional information, the additional information coming from subjects, alteration declarations or answering to the awareness documents and different information case by case, which we made possible to manage effectively due to an internal organization and a systematic work.

Since January 2013 it became functional a new operating system of online application and registration of personal data controllers.

The Registration Department during the period June 2012 - June 2013 has issued **2214** awareness official letters addressing the controllers, urging the exercise of the legal duty to notify under Articles 21-26 of the Law. The grand total of these official letters sent to both public and private controllers is about **16315.**

As a result of this awareness strategy and legally binding as well, during the period June 2012-June 2013 at the Commissioner's Office have submitted their notifications **1299** controllers. The total number of data processing reports by the controllers on the territory of the Republic of Albania has reached 3950 reports.

Moreover, thanks to its policy and strategy on helping and assisting the controlling entities that notify, an important number of controllers that were calling our offices, have been attended on purpose of clarification and assistance as well as telephonic communications were performed.

We have assisted through telephone around 253 subjects which have called our offices or requested assistance and also attended for clarifications and assistance around 134 controllers.

- **Identification and information about the cases that constitute a violation of privacy and personal data.**

In the framework of cooperation with the Inspection Department, in order to increase the number of reports, but also for the more rigorous application of the law when its provisions are violated, we have regularly informed this Department of the subjects whose official letter was sent to and who does not have announced in the deadlines set, by unfulfilling the obligation to notify, and also of the subjects who did not meet and specified the declared information, which constitutes an administrative offense.

Also, pursuant to the provisions on "Preliminary control" and to the general provisions, based on the reports of income through notification form, we exchanged and interacted among the KMDP's bodies, information to identify the cases that constitute a breach of privacy and may be subject to further verification, administrative investigations, inspections, making recommendations or in administrative violation and sanctioned with a fine;

- **In the framework of the EU - IPA 2009.**

In the context of the project "Support to the Commissioner for the Protection of Personal Data (KMDP) with Training of Data Protection Officers in the Albanian Public Sector", in cooperation with experts of the project, we participated in the workshop; "**Management of the systems of personal data archiving and SMSI generally** " where the Registration Department referred on the topics of the preliminary control procedures. Furthermore, in collaboration with the project

expert Stefan Szyszko was prepared and finalized the material: **Communication channel between KMDP and the Persons of Contact**.

The purpose of this document is to provide a separate and steady contact channel within the KMDP in order to consult the Persons of Contact related to the problems concerning the interpretation of the law on data protection, which they face in the course of their duties. Through this channel, the Persons of Contact will be aware of who and how to direct their inquiries.

- **The Data Protection Day**

On January 28, on the occasion of the European Day of Protection of Personal Data, The Commissioner for Personal Data Protection organized several activities like:

a) Open Day where citizens were invited to visit the Authority and have some informative materials about Data Protection

b) The Commissioner for Personal Data Protection signed a cooperation agreement with the Rector of the University of Tirana.

c) In the 9-year school "Edith Durham" students of the school presented their creativity in pictures on the topic "Protect your Privacy".

- **Raising Awareness Campaign**

- On 7 June 2012, a seminar titled "Cloud Computing phenomenon and Protection of Personal Data" was held at the premises of the Commissioner for Personal Data Protection. Dr.Stefan Szyszko, a short-term expert from Poland within the project entitled "Consolidation of the Office of the Commissioner for Data Protection in Albania", was referring to the seminar as one of the prominent experts in the field. This workshop aimed at raising awareness of data subjects and controllers representatives on Cloud Computing phenomenon and personal data protection.
- On 21 June 2012, at the premises of the Commissioner for Personal Data Protection, a seminar titled "Protecting Privacy and the Right of access to official documents, two rights in conflict with each other?" was organized in cooperation with IPA 2009 Project titled: "Consolidation of the Commissioner for Data Protection in Albania". Speaker at the seminar was renowned British expert in the field of data protection Mr. Graham Sutton, who also helped in the preparation of the Albanian personal data protection law. At this event open to the public were present representatives from: the Council of Ministers, the General Prosecutor, HIDA, HJC, Euralius, The European Union Delegation, Commissioner for Protection from Discrimination, General Directorate of Civil Status, the General Police Directorate etc.

- In the framework of cooperation between IPA 2009 Project "Consolidation of the Commissioner for Data Protection in Albania according to EU standards" (Europe Aid/129606/C/SER/AL) and the Commissioner for the Protection of Personal Data, on date 20 September on the premises of "Hotel International" a seminar was organized on "Drafting Laws which include the subject of Protection of Personal Data". In this workshop, in which the participants were representatives of the legal departments of all ministries and subordinate institutions, presentations were made by experts of an international level in the field of personal data protection and legal drafting technique, as

Ms.Waltraut Kotschy, former Commissioner of the Council of Europe and the former Austrian Commissioner for Data Protection and Mr. Jose Lopez Calvo, deputy-Commissioner of Spanish Data Protection Authority.

- Awareness raising activities on the protection of personal data with the citizens of Shkodra, Vlora, Durres and Fier. During 2012, the Commissioner for Personal Data Protection, in collaboration with the assistance of the IPA 2009 Project entitled "Consolidation of the Office of the Commissioner for Data Protection in Albania", organized four awareness activities with citizens, subjects of personal data protection law, in the cities of Shkodra, Vlora, Durres and Fier. These awareness activities were attended by representatives of the Commissioner for Personal Data Protection and the IPA project, who shared key messages with various citizens in regard to the preservation of privacy and personal data protection.

- During this period the Authority of the Commissioner has organized a series of workshops with the representatives of the educational institutions and other public controller in connection with legal obligations arising from the implementation of the Law on Protection of Personal Data and the latest developments in the field of privacy. These seminars was held during this period in the districts of Kruja, Peshkopi, Vlore, Fier, Elbasan, Kukes, Saranda, Gjirokastra, Lezha, Durres, Berat, Përmet and Tirana.

- The Authority of the Commissioner trained over 60 the representatives of local institutions about the Law on Protection of Personal Data and the obligations arising from its implementation. These meetings were organized by the Commissioner for Personal Data Protection in collaboration with the Prefecture of Tirana.

- On February 15, Mrs. Flora Çabej (Pogaçe) the Commissioner for Personal Data Protection, hosted a group of students from the Masters in Political Science at the University of Tirana and talked with them about the right to protect personal data.

- On the 26 of April 2013, the Commissioner for Personal Data Protection together with the Faculty of Law Project and with the assistance of the EU project "Support to the Commissioner for Personal Data Protection (KMDP) with training of data protection officers in the Albanian on public sector "organized the Conference" New Dimensions in Privacy Law "with the participation of about 240 students from the Faculty of Law. For participants were distributed certificates.

- During these period it has been organized Awareness meeting with teachers and senators of school 9 years school "Osman Myderizi" Tiranë, “Gjon Buzuku” Tiranë, Dora d’Istria” Tiranë and “Nonda Bulka” Përmet. These awareness meetings had their focus on addressing the risks of violation of privacy when using the Internet and the use of information technology in general.

- In December, representatives of the Commissioner's Authority in collaboration with the High School "Çajupi" organized an awareness meeting with the school’s senators, in order to sensitize them on the crucial area of personal data protection. Specialists of the

Commissioner's Authority made a presentation of the field of personal data protection, focusing at the side effects that may be caused to young people using social networks.

- **Media**

The Commissioner Flora Çabej (Pogaçe), has published an article on October 2012 in the prestigious journal "Privacy Laws & Business International" entitled "Albania amended the Law on the protection of personal data in order to reflect the European Directive".
Another important article about the importance of protecting the personal data were also published in two main Albanian daily newspapers "Mapo" and "Shekulli".
The Commissioner for Personal Data Protection gave to A 15 print, audio visual and electronic media Recommendations, about the publication of personal data of the Albanian citizen F.P.

During this year, representatives of the Commissioner has given several interviews and made a few presences in television talk shows speaking in general about the right to protect the personal and in particular about the risks of protecting privacy when using the Internet or the publication of personal data in the media etc.

- **International Cooperation**

- The Commissioner for Personal Data Protection in October 2012, attended the Regional Balkan Conference of Commissioners for Personal Data Protection, organized by the Commissioner of Montenegro in Budva city. The main topic on the agenda was "Access to Information and Protection of Personal Data". This conference aimed on exchanging experience in the field of the right to access to information and the right to personal data protection, enhancing regional cooperation in this field and the union of these rights in one authority.

- The Commissioner Authority took part in November at the 6th Conference of the Association of Authorities for Personal Data Protection of Francophone countries, which took place in Monaco. The conference at its opening was greeted by the Prince of Monaco Albert II, who stressed the importance of the protection of personal data in the Principality of Monaco since the country adopted in 2008 the new Law on the Protection of Personal Data and the importance of sharing experiences in face of the challenges and difficulties in the field of personal data protection in the francophone area.

- Earlier in October, within the Francophone Cooperation, Albanian Authority for Personal Data Protection, by request of the Association of Francophone Authorities for Protection of Personal Data was represented at the Conference of the Association of Ombudsmen and Mediators of Francophone countries (AOMF) on the Rights of Children which was held in Tirana on 23 and 24 October 2012. In this conference, Commissioner for Personal Data Protection presented the works of Francophone Association and the Albanian authority, in connection with measures taken to protect the privacy of children when using the Internet. Also we have had constant contact with the Association of Francophone Authorities for the Protection of Personal Data in connection with the exchange of experience and best practices in the field of personal data protection.

- The Commissioner for Personal Data Protection took part in the 15th meeting of the Authority for Personal Data Protection of Central and Eastern Europe held in Belgrade (Serbia), from 10 to 12 April 2013. The meeting addressed three sets of issues, to which representatives of the authorities for personal data protection presented their experiences. These include: data security, data processing in the field of employment and independence of authorities for personal data protection and the challenges they face.

- The Croatian authority for the protection of personal data with the assistance of TAIEX organized the conference "Protection of Personal Data and Internet-New Challenges" which was held in Zagreb (Croatia) on 20 and 21 June 2013. The meeting was attended by the representatives of the authorities of the Personal Data Protection including: Serbia, Bosnia-Herzegovina, Montenegro, Ukraine, Croatia, Albania and Macedonia. The Albanian Commissioner for Personal Data Protection presented his experience on the internet penetration in the country and the consequences that come from a misuse of it, also citing measures taken in case of breaches of personal data.

➢ **Others**

- In March, the EU Project “Support to the commissioner for the protection of personal data (CPDP) with training of data protection officers in the Albanian public sector” concluded their training process about the trainers of trainees. The course trained 10 employees of the Authority of the Commissioner and gave them the relevant certificates.

- On the 6 of June the representatives of the Public Administration of central and subsidiary institutions completed two months training organized and funded by the EU project “Support to the Commissioner for Personal Data Protection (KMDP) with training of data protection officers in the Albanian on public sector ". A finale event was organized in the office of the Authority and during the event the Project distributed the certificates for the participants.

- The Commissioner for Personal Data Protection has opened an official profile of the Commissioner for Personal Data Protection at the social network “Facebook”.

- On the 29 of April, the Commissioner held a Web conference with representatives of social network Facebook based in Ireland which is also the headquarters of the company covering Albania. The web conference was run by two managers of the Company and was attended by the entire staff of the Commissioner.

- 12 students from the Law Faculty, University of Tirana have concluded their internship at the Authority of the Commissioner for the protection of the personal data.

- It’s conceived and designed the first number of the “Law and Privacy periodical magazine, of the Authority of the Commissioner.

- It is taken over the controller’s notification system. The system is located in the physical environment of the Commissioner Authority and it is related to the Authority’s portal to get the applications of the notifications of the controllers and enables the publishing of the open registry.

ANDORRA / ANDORRE

Développements majeurs intervenus en Andorre depuis la dernière réunion plénière du T-PD

Llei 28/2012, del 18 d'octubre, de modificació de la Llei del joc del bingo, del 28 de novembre de 1996, modificada per la Llei del 15 de novembre del 2001 qui précise le contrôle d'admission des joueurs

Decret del 14-11-2012 d'aprovació del Reglament que regula els serveis de salut laboral qui réglemente les services de santé au travail et la surveillance de la santé des salariés

Decret del 6-03-2013 pel qual s'aprova el Reglament del registre d'ocupació d'allotjaments turístics (ROAT), qui contient des dispositions relatives aux traitements d'informations nominatives entre les hébergements touristiques el le Ministère de l'Intérieur dans le cadre de la Sûreté Publique.

Llei 2/2013, de 18 d'abril, de la funció de l'estadística pública, qui fixe les objectifs, l'organisation et les règles de fonctionnement de la stadistique publique et des informations collectées au moyen d'enqêtes statistiques.

AUSTRIA / AUTRICHE

Major developments in the data protection field in Austria

In response to your e-mail of 19 June 2013, the *Datenschutzkommission* (Austrian DPA) submits the following facts:

1. Following the judgment of the European Court of Justice (EJC) of 16 October 2012, case C-614/10, in which the ECJ declared that by failing to take all of the measures necessary to ensure that the legislation in force in Austria meets the requirement of independence with regard to the *Datenschutzkommission* (Data Protection Commission), the Republic of Austria has failed to fulfil its obligations under Art. 28 of Directive 95/46/EC, the Austrian Data Protection Act 2000 (*Datenschutzgesetz 2000*) was amended in order to ensure "complete independence" of the *Datenschutzkommission*. The relevant amendment was published in Bundesgesetzblatt (Official Journal) I Nr. 57/2013 and entered into force on 1 May 2013.

2. The *Datenschutzkommission* as the competent Austrian Data Protection Authority will be replaced by the *Datenschutzbehörde* by 1 January 2014. Just like the *Datenschutzkommission* the *Datenschutzbehörde* will fulfil all requirements of Art. 1 of the Additional Protocol to Convention 108 and of Art. 28 of Directive 95/46/EC. The replacement is a consequence of the establishment of Administrative Courts which will deal with appeals against decisions of administrative authorities. A decision of the *Datenschutzbehörde* will consequently be subject to judicial review by the future *Bundesverwaltungsgericht* (Federal Administrative Court) and then of the *Verwaltungsgerichtshof* (High Administrative Court) and the *Verfassungsgerichtshof* (Constitutional Court). Currently, decisions of the *Datenschutzkommission* are only subject to judicial review by the *Verwaltungsgerichtshof* and the *Verfassungsgerichtshof*.The relevant amendment of the Austrian Data Protection Act 2000 was published inBundesgesetzblatt I Nr. 83/2014 and will enter into force on 1 January 2014.

3. The Datenschutzkommission decided on 18 January 2013 to submit to the EJC the following questions concerning the interpretation of the Data Retention Directive 2006/24/EC for a preliminary ruling: *Is Article 7(c) of Directive 2006/24/EC 2 to be interpreted as meaning that natural persons affected by the retention of data within the meaning of the Directive do not fall into the category of 'specially authorised personnel' within the meaning of that provision and may not be granted a right to receive information on data relating to their own person from the provider of a publicly available communications service or a public communications network? Is Article 13(1)(c) and (d) of Directive 95/46/EC to be interpreted as meaning that the right of natural persons affected by the retention of data within the meaning of Directive 2006/24/EC to receive information on data relating to their own person pursuant to Article 12(a) of Directive 95/46/EC from the provider of a publicly available communications service or a public communications network can be excluded or restricted? If Question 1 is answered at least partly in the affirmative: Is Article 7(c) of Directive 2006/24/EC compatible with the fundamental right laid down in the second sentence of Article 8(2) [of the Charter of Fundamental Rights of the European Union] and thus valid?*

This decision is available (in German) at http://www.dsk.gv.at/DocView.axd?CobId=50274. The case is pending at the EJC, the case no. is C-46/13.

17. July 2013

Austrian data protection commission
The Executive Member:
SOUHRADA-KIRCHMAYER

BELGIUM / BELGIQUE

Voici les 2 développements majeurs intervenus en Belgique dans le domaine de la protection des données :

- Juin 2013 : Protocole d'accord entre le Service public fédéral Justice et l'autorité indépendante de protection des données belge afin de permettre aux entreprises établies en Belgique d'échanger plus facilement des données à caractère personnel avec les entreprises partenaires établies en dehors de l'UE.

  L'échange transfrontalier de données à caractère personnel au sein de l'UE ne pose pas de problème. Par contre, l'échange de données en dehors de l'UE n'est en principe autorisé qu'avec des pays garantissant un niveau de protection adéquat. Dans la pratique, ce niveau est évalué par la Commission européenne.
  Il est néanmoins possible pour les entreprises établies en Belgique de transmettre des données à caractère personnel à ces pays si les garanties nécessaires sont établies dans des clauses contractuelles spécifiques également appelées "clauses contractuelles types" de la Commission européenne.

  Concrètement, les entreprises souhaitant transmettre des données à caractère personnel à des entreprises partenaires en dehors de l'UE doivent établir un contrat avec ces entreprises. Ce contrat peut être un des modèles-types de la Commission européenne mais cela n'est pas obligatoire. Les conséquences pour la validation du contrat diffèrent toutefois selon qu'il s'agit d'un contrat-type ou non et sont déterminées dans le protocole d'accord rédigé par le SPF Justice et la Commission de la protection de la vie privée :

  - un contrat conforme à un modèle de l'UE doit uniquement être soumis à la Commission de la protection de la vie privée afin d'en vérifier la conformité avec le modèle-type de l'UE. En cas de conformité, l'échange de données à caractère personnel sera accepté ;
  - un contrat qui diverge du modèle-type de l'UE doit être présenté à la Commission de la protection de la vie privée afin d'en évaluer les garanties relatives à la vie privée. Si ces garanties satisfont aux conditions du protocole d'accord, le contrat doit ensuite être sanctionné par arrêté royal via le ministre de la Justice.

  L'autorité indépendante de protection des données belge est très satisfaite du protocole d'accord car il offre une plus grande sécurité juridique à la fois aux personnes dont les données sont transmises et aux entreprises concernées. Il s'agit d'un grand pas en avant dans la protection des données à caractère personnel et d'une application efficiente de la loi relative à la protection de la vie privée.

  Ce protocole permet de déterminer les conditions auxquelles les clauses contractuelles doivent satisfaire et d'établir les procédures d'autorisation d'échange de données avec des pays dont le niveau de protection des données n'a pas été reconnu comme adéquat. Ce protocole réduit fortement les formalités administratives pour les entreprises et garantit des normes élevées de protection de la vie privée pour les données de nos entreprises belges échangées avec des pays tiers.

- Aout 2012 : Cyber-surveillance : En juillet 2011, l'autorité indépendante de protection des données belge a lancé une consultation publique sur le contrôle électronique sur le lieu de travail, impliquant toutes les parties concernées. La consultation publique s'est

clôturée par une après-midi d'étude le 16 décembre 2011, dont l'ensemble des réactions et des réflexions suscitées a ensuite été compilé par l'autorité indépendante de protection des données belge dans une grande recommandation unique. Afin de concentrer les informations essentielles pour le grand public, l'autorité indépendante belge en a extrait une brochure d'information composée d'un texte introductif général et d'une série de questions fréquemment posées. La brochure d'information est disponible sur le site de l'autorité indépendante belge en format pdf dans le dossier thématique "Cybersurveillance". (www.privacycommission.be)

CYPRUS / CHYPRE

Since T-PD Plenary meeting held in June 2012 the only major development in the field of Data Protection was the entry into force of the Amendment Law, Processing of Personal Data (Protection of Individuals) Law 2012 (L.105(I)/2012).

The most important amendment introduced by the Law is the increase of the monetary penalty from 8.540 euro to 30.000 euro.

The Office for Personnal Data Protection

Czech Republic

Personnal Data Protection development

September 2013

New duty introduced by the Government will be systematically adhered to starting next year, specifically that the impact on privacy will be evaluated by the time that each new legal regulation is submitted. This will prevent situations where the possible drawbacks related to personal data protection are ascertained only after the given laws and regulations have already been adopted.

The Government adopted modified legislative rules with a new **duty to evaluate the impact of individual draft laws on the protection of privacy and personal data**, not only in drafting substantive intentions of laws, but also of explanatory memoranda.

In the area of **electronic communications** the Office welcomed the Government draft amendment to the Electronic Communications Act, the Code of Criminal Procedure and some other laws, which was concerned exclusively with **maintenance and utilisation of traffic and location data for electronic communications**.

Traffic and location data are newly defined in the Electronic Communications Act on the basis of the informative value of the individual data. As a rule, the recipient of an electronic communications service whose identity is known to the court or prosecuting body will be subsequently informed ex officio of any order for determination of these data.

Development of the "ORG Information System"

The basic aim of the ORG Information Systém (started in 2011) is to provide for protection of personal data within the entire system of the Basic Registers (**Register of Inhabitants** – updated reference data on citizens of Czech republic, foreigners with residence permit or incomers who were granted asylum here; **Register of Rights and Duties** – the data of competency of public administration offices; **Register of Persons** – the reference data about corporations, enterprising individuals or public authorities; **Register of Territorial Identification, Addresses and Real Estate Property** – data on the basic territorial elements, for example territories of the states, regions, municipals or parts of urban areas, plots and stress; **Information System of Basic Registers** – the four registers operate in its framework) by means of replacing the current use of the birth identification number as a universal identifier of natural persons with a system of meaningless identifiers. These identifiers will differ for the individual agendas or groups of agendas and will thus not allow to search for information on a natural person in a different agenda based on knowledge of one identifier. The privacy is

upgraded, among other things, due to the fact that the system handles not with the real personal identification number but only with randomly generated identifier.

This issue is in charge of The Office for Personal Data Protection by means of **Individual Identifiers´ Converter.**

The only place where all identifiers are stored is the ORG Information System. However, this system does not contain any names of natural persons and, therefore, even knowledge of all identifiers does not enable the Office for Personnal Data Protection, who is responsable for the ORG Information Systém, to determine how they are assigned to the individual natural persons. In this way, implementation of the project of Basic Registers substantially contributes to protection of personal data of citizens.

The Office for Personal Data Protection has published the **handbook** (the English version on-line) **of** offering a **methodology guidance for video surveillance** systems operators to help them meet the obligations ensuing from the Personal Data Protection Act.

Information bulletin

As part of our annual "My Privacy! Don't Look, Don't Snoop!" contest, we tried to ask young people whether they know how to make use of privacy protection possibilities offered to them on the most personal data hungry network: Facebook. The responses that we received we are adding to the special issue of the Information Bulletin as an inspiration: The Bulletin will be devoted mainly to teachers - of course, parents are not precluded.The Buletin was distributed with the Student Diary (8 000 schools). The contributions that we have included in the 2013/2014 Student Diary "Good Advice is More Valuable than Gold! How to Protect Your Privacy on Facebook" may help with this.

Discussion with large scale of professionals who contributed to special Information bulletin to be continued in January 2014 to open the topic "PDP at school and in educational process".

The Office for Personal Data Protection is a party to a greatmany **court proceedings.** As far as findings from the decision-making practice in 2012 are concerned, mention should be made of five important areas related to **tax administration, the nature of an instigation or complaint by the data subject, consent of the data subject to personal data processing, the notion of commercial communication and operation of camera surveillance systems.**

Tax administration

Frequent arguments related to the actual application of the Personal Data Protection Act in the area of tax administration refer to the exemption embodied in Article 3 (6) (f) of the Personal Data Protection Act, according to which Articles 5 (1), 11 and 12 do not apply to processing of personal data necessary for the performance of the controller's duties stipulated by the special laws in pursuit of an important financial interest of the Czech Republic or the European Union, including, in particular, the stability of the financial market and currency,functioning ofmoney circulation and payment relationships, as well as budget and fiscalmeasures.

Court in Prague stated that *"it cannot be stated in general that the Personal Data Protection Act does not apply to tax proceedings."* The assessment of whether the said exemption applies to a certain situation in view of an important financial interest of the Czech Republicshould be made in co-operation with the Office for Personal Data Protection and the kompetent tax authority.

It has also been argued in the said context that the tax rules contain a special autonomous legal regulation of confidentiality, affording a higher level of protection to all data being processed and *"that the non-disclosure duty borne by the tax authorities is limited in a situation where the tax authority is requested to provide data by an entity authorised to obtain such data, which in the given case ... is the Office for Personal Data Protection, which is authorised to become acquainted with personal data and is also bound by the duty to maintain confidentiality."*

Performance of supervision

A petitioner is not entitled to claim that the Office exercise its supervisory competence and the relevant pleading is thusmerely an instigation to exercise the Office's supervisory rights, where information from the Office on the manner of resolving an instigation is merely a communication from the Office, rather than a decision pursuant to Article 65 of Act No. 150/2002 Coll., the Code of Administrative Justice.

Consent of the data subject to personal data processing

In a case that ultimately resulted in a judgment rendered by the Municipal Court in Prague, the court assessed **processing of personal data of a job seeker**, which continued after the end of the selection procedure for the vacancy without express consent of the data subject.

Commercial communication

An individual response to a specific offer is not an unsolicited commercial communication pursuant to Act No. 480/2004, on certain services of the information society and on amendment to certain laws (the Act on Certain Services of Information Society) and the same is true of a specific counterproposal in reaction to an offer following from an advertisement.

Operation of camera surveillance systems

In the judgment, the Municipal Court in Prague stated that where a camera surveillance systems used extensively, i.e. where it simplymonitors the premises where the clients of a hotelare present, rather than being, e.g. focused on objects that could be the aimof unlawful conduct (such as places intended for storage of things), the specific manner of obtaining camera recordings cannot be deemed to comply with the requirement of Article 5 (2) (e), the part of the sentence after the semicolon, of the Personal Data Protection Act, i.e. respecting the right of the persons being recorded to the protection of privacy and personal life.

The said manner of installation of the camera surveillance system is, in the court's

opinion, clearly disproportionate. Indeed, the interest in protection against minor thefts, vandalismand potential unlawful conduct by a certain party cannot automatically overweigh the interests in protection of privacy and personal life.

ESTONIA / ESTONIE

Major developments in the data protection field

There have been no major developments in the field of protection of personal data in Estonia during June 2012 – July 2013.

However, we would like to point out that we celebrated the Data Protection Day. The 2-day international conference Ethical Dimensions of Data Protection – Global and Local Challenges was organised together with The Centre for Ethics of the University of Tartu.

Estonian Data Protection Inspectorate

July 12, 2013

12.8.2013

INFORMATION ON THE MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD IN FINLAND SINCE THE T-PD PLENARY MEETING HELD IN JUNE 2012

Legislation

The Biobank Act was confirmed by the President of Republic in November 2012 and the regulation will come into force in September 2013. The Act sets new standards on research use of samples of human origin.

The activity of the Data Protection Ombudsman

In Data Protection Day 28.1.2013 The Data Protection Ombudsman participated in the data protection occasion organized by Nokia Plc and the office of Data Protection Ombudsman and he also issued the press release about data protection in order to raise awareness and respect of data protection among controllers and general public as data subjects.

The Data Protection Ombudsman has also published a sector survey on regular customer systems that was implemented early in the year[1]. It found out that the legal quality of regular customer systems varies to some extent. Some of the respondents could not say why they use a regular customer system.

At the request of the Data Protection Ombudsman, the Data Protection Board commented the strong identification system required in some booking systems. The case referred to the legal quality of an online service of an optician store chain where people booked appointments and implemented other actions using their name and social security code. The Board agreed with the Ombudsman's statement that the system in question is not secure enough and social security codes are being used to separate people from each other in databases. The controller in question has started to repair the system.

At the request of the Data Protection Ombudsman, the Data Protection Board studied CCTV monitoring in the stairwells of residential buildings as an important matter of principle. The case referred, among other things, to the link between the Personal Data Act and the Criminal Code of Finland. The Board stated as its opinion that CCTV monitoring is possible also in these facilities based on the stipulations of the Personal Data Act.

The Data Protection Ombudsman has also referred to the Data Protection Board cases on exercising right of access and credit information. In the first case, the main question was whether the right of access as required by the Ombudsman should also be possible by means of an electronic signature. The latter case referred to the way the information in the credit information register is being used, its availability in the manner regulated by the Credit Information Act and also the correctness of the information provided to the registered people.

[1] Sector survey is a tool that the Data Protection Ombudsman has developed. Its goal is as efficient inspection activities as possible utilising technological means.

The Data Protection Ombudsman also assisted the consumer protection authority in determining policies on the legal nature of services based on geographical information that are funded by means of advertisements. In this case, the key question was the link between contractual terms and consent.

One important reform that received fairly little attention was the implementation of employee tax numbers. In Finland, each person is issued a social security code (HETU) that is entered in the Population Register and an electronic ID to be used when dealing with the authorities (SATU). Furthermore, the Tax Administration has now implemented a tax number issued to all employees in an attempt to curb the grey market. At least in this respect, the public administration seems to manage the risks pertaining to the management of identities. On the other hand, the development of mobile services based on SATU has had a fairly slow start.

Another step forwards by the public administration is the development regulated by the Act on Public Data Administration that entered into force in 2011: the control on the utilisation of information technology has been further centralised to the decision-makers of state-owned enterprises. One of the proposals issued over the course of the year was establishing an IT service company owned by the State. The national auditing based on the Data Security Decree seems to have started well.

The Office of the Data Protection Ombudsman participated in the control of the above-mentioned issues and the control of scientific research, supervision of DNA sample collections, issues pertaining to intelligent transportation systems and road tolls, communication on threatening data leaks from smart phones, reform of the Act on Processing Personal Data by the Police, the work of the Human Rights Committee, and many other projects.

FRANCE

Action de la CNIL en faveur de l'éducation au numérique

La CNIL entend proposer au Gouvernement de faire de l'éducation numérique la grande cause nationale 2014. Un collectif pour l'éducation numérique a été créé dans ce dessein. Il est composé de 42 organismes issus du monde de l'éducation, de la société civile, de l'économie numérique, ainsi que d'institutions nationales et internationales.

L'objectif poursuivi par la Commission est à la fois de promouvoir une approche globale et de développer une véritable pédagogie du numérique afin d'assurer un univers numérique respectueux des droits et libertés ainsi qu'une autonomie et une responsabilisation du citoyen dans ses usages et sa maîtrise de cet environnement.

Le collectif créé a défini cinq propositions communes très concrètes :

1. Lancer un événement d'envergure nationale sur l'éducation au numérique (journée éducation au numérique ou « cafés numérique »).

2. Créer une plateforme collaborative de contenus disponibles en ligne gratuitement (glossaire animé, MOOC, etc.).

3. Réaliser et diffuser des formats courts en partenariat avec France Télévisions (formats courts éducatifs, fictions, web séries).

4. Créer des modules d'éducation au numérique destinés aux enfants de 6-12 ans.

5. Lancer des actions de sensibilisation au numérique à destination des entrepreneurs

Plus largement, la Commission a associé le Conseil de l'Europe à ses travaux et un projet de résolution sur l'éducation numérique a été soumis et adopté lors de la dernière Conférence internationale des commissaires à la vie privée, à Varsovie.

GERMANY / ALLEMAGNE

Developments in the field of data protection at national level in 2012/2013

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

After almost three years the Study Commission on the Internet and Digital Society established by the German Bundestag in 2010 completed its work. On 18 April 2013, the 17 Members of Parliament and 17 experts submitted their findings and recommendations to the Parliament, addressing privacy and data protection rights on the Internet in detail.

Please go to http://www.bundestag.de/internetenquete/index.jsp for further information - in German - concerning the study commission and the interim reports compiled by it.

2. International Conference of Data Protection and Privacy Commissioners

The Federal Ministry of the Interior invited 250 experts from the research and the business communities, the EU Member States and the data protection supervisory authorities to a conference in Berlin on 17/18 October 2012.

The conference identified particular data processing risks in the private sector and discussed further regulatory approaches.

Apart from stricter regulations geared to specific threats to the personal rights of individuals the conference primarily dealt with appropriate regulations for individuals.

The conference results are helping push ahead the reform of European data protection law.

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 Technikwissen-schaften) selected the winner of the contest launched to gather ideas on how to limit the shelf-life of Internet content, completing the one-year contest.

School children, university 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 submitted the Draft Act to Regulate Data Protection in the Employment Sector, which has since been removed from the negotiation agenda of the German Bundestag owing to diverging views of employers and trade unions with regard to major aspects of the draft. As it will take time to reconcile those views, the legislative procedure will not be completed within this legislative period.

5. Data Protection Foundation

In January 2013, the Federal Government established the Data Protection Foundation (Stiftung Datenschutz), which is mandated to

- look at whether products and services comply with data protection needs,

- enhance data protection education,

- to make users more aware of data protection measures which they can take to - protect their data and

- develop a data protection audit.

The Data Protection Foundation is a non-profit foundation with legal capacity under civil law, and is seated in Leipzig -(Karl-Rothe-Straße 10-14, 04105 Leipzig, phone 0341/ 5861 555-0, fax 0341 / 5861 555-9, info@stiftungdatenschutz.org).

The foundation has received €10 million in assets from the federal budget; furthermore it receives an annual amount of €205,000 from the Federal Interior Ministry's budget.

6. Federal Government report pursuant to Section 48, first sentence, no. 1 of the Federal Data Protection Act (BDSG) on the impacts of Sections 30a and 42a of the Federal Data Protection Act

Section 30a accommodates the particularities of commercial market or opinion research as opposed to marketing. Commercial market and opinion research uses scientific methods and techniques to supply public- and private-sector clients with information they need as an empirical basis to assist with economic, social and political decision-making.

Section 42a of the Federal Data Protection Act requires private bodies and public bodies of the Länder in so far as they participate in competition as public-law enterprises to report the unlawful access to personal data in all cases where specific and particularly sensitive personal data have been unlawfully transferred or otherwise unlawfully disclosed to third parties with the threat of serious harm to the data subject’s rights or legitimate interests. Section 42a serves to contain the damage data protection breaches caused particularly to data subjects, and to make businesses more inclined to secure those data.

The Federal Government Report states that Sections 30a and 42a have proved their worth.

The Federal Government does not at present recommend amending the provisions.

A provision along the lines of Section 42a has been introduced in Section 83a of Social Code Book X for social assistance funds under public law.

7. DE-Mail Act

On 3 May 2011 the Federal Government adopted the “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 electronic mailing systems. The new provisions and the technical guidelines governing DE-Mail provide the necessary framework conditions to create legal certainty for the use of such messages. DE-Mail has been implemented 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. De-Mail providers must submit a data protection certificate issued by the Federal Commissioner for Data Protection and Freedom of Information (BfDI). So far, the following businesses provide DE-Mail services: Telekom Deutschland Ltd., T-Systems International Ltd., 1&1 De-Mail GmbH, and Mentana Claimsoft Ltd.

8. The new identity card

On 1 November 2010, the new identity card was launched in Germany.

It enables card holders to prove their identity - safely and unequivocally – when using the Internet or vending 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 protection mechanisms EAC (Extended Access Control), BAC (Basic Access Control) and PACE (Password-Authenticated Connection Establishment), 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 authorization 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.

9. 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 tracking of mobile end-user devices) 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 telecommunications services.

10. Cloud computing

In 2011, the Federal Ministry of Economics and Technology launched a technology programme called “Trusted Cloud”. By 2015, 14 innovative, secure and legally compliant cloud solutions will be developed and tested in various application fields. At the same time, the Ministry of

Economics has set up the Trusted Cloud Competence Centre, which brings together various working groups, including one addressing the legal framework conditions of cloud computing. The working group is led by Prof. Georg Borges and brings together experts from the business and scientific communities and from data protection authorities. Data protection is one of the top issues, along with copyright matters, contractual law and liability issues. As regards protection of data involved in cloud computing, the working group has submitted a proposal regarding fit-for-use obligations to check those processing data on behalf of the controller.

11. IT summit

The Internet with its great opportunities and many risks has an increasing influence on our professional and private lives, giving rise to urgent privacy and security issues. The IT summit working group "Trust, data protection and security on the Internet" therefore dealt with how to take on those issues, addressing above all cloud computing, security of electronic identities and mobile security. The working groups, which met several times during the summit period with the involvement of federal ministries, business representatives, data protection commissioners and consumer associations, presented their findings at the National IT summit held in Essen on 13 November 2012.

“Since June 2012 there have been two legislative changes in the Greek Data Protection Act (law no.2472/1997). The most important is included in law no.4139/2013, which is the basic Greek law on drugs. Its Art. 79 amended Art.2 of the Data Protection Act, in particular the conditions for publication in the press of still pending criminal cases. The law now clarifies that such publication is permitted only in relation to specific crimes and after a relevant permit by the Attorney General office has been granted; such permit must also set the manner of publication as well as its time period. The reason for such publication may only pertain to the protection of the public and in order to facilitate the prosecution process. The individuals affected have the right to appeal – a process that must be concluded within a very short period of time. This amendment comes as the legislative response to, and indeed follows closely, the Greek Data Protection Authority Decision no. 128/2012 on the publication in the press of the personal information of several HIV-positive women.

In addition, law no.4152/2013 extended the exemption basically granted to court authorities on the notification obligation for the processing of common personal data and on the prior permit for the processing of sensitive data while in the course of executing their duties (Art. 7a) also to the Inspectors-Controllers Body for Public Administration (ICBPA)”.

HUNGARY / HONGRIE

Country report
(January 2013 – up to now)

1. Major legislative changes

The most relevant innovation of the Act CXII of 2011 on Informational Self-determination and Freedom of Information (hereinafter referred to as Infotv.) is the introduction of the ***data protection audit***. The data protection audit is a *service provided by the National Authority for Data Protection and Freedom of Information* (hereinafter referred to as NAIH) designed to evaluate and assess data processing operations in progress or proposed along technical merits, intended to effectively implement a high level of data protection and data security system. Proposed data processing operations may be audited if deemed justified based on the maturity of the data processing strategy. Data protection audits are conducted by the Authority at the data controller's request. For the data protection audit *an administrative service fee shall be charged* in the amount decreed by the relevant minister.
The Authority shall record the results of the data protection audit in an *audit report*. The audit report may also contain recommendations for the data controller.

Another major amendment – in effect as of 30th March 2013 – to the Infotv. was put in place by inserting para. (5) into Section 4 of the Act as follows:

(5) The principle of lawfulness and fairness shall be considered satisfied in connection with the processing of personal data where a person wishing to learn about the data subjects opinion visits - within the framework of freedom of speech - the data subject at his/her home or residence, provided that the data subjects personal data is processed in accordance with the provisions of this Act and the poll is taken for reasons other than business purposes. Such visits may not be carried out on days designated as public holidays by the Labour Code.

The third legal modification worth mentioning is that – as of 1st July 2013 – the data processor is permitted to subcontract any part of his operations to another data processor.

2. Hot issues – with relevant public impact

2. a) *Google Street View (GSV)*

Following numerous consultations with the representatives of Google Inc. (service provider of GSV) and several investigations carried out by the former Data Protection Commissioner dated back to 2009 as well as taking into consideration the recent rulings (C-468/10. and C-469/10.) of the ECJ the NAIH issued a statement in which it approved the launch of GSV service in Hungary provided the Google complies with the relevant data protection principles and preconditions (including, among others, prior notification to the public; enabling for data subjects to submit requests for deletion; blurring of personal data as soon as possible etc.) set forth by NAIH in its statement.

2. b) *Application of CCTV devices in workplaces*

Numerous petitions were received by both the NAIH and the former Data Protection Commissioner (hereinafter referred to as DP Commissioner) in recent years in which the applicants complained about the widespread application of CCTV surveillance devices in workplaces.

From 2012 on both the former Labour Code and DP Act of 1992 have become repealed by new legal instruments. The new Labour Code, effective as of 1st July 2012, already includes governing provisions (§§ 9 and 11) that are to be taken into consideration as for CCTV devices in workplaces. These general provisions can lead, however, to different enforcement of the right of informational self-determination.

As a result of a thorough investigation we issued a recommendation in which we proposed guidelines to the employers with the objective of enabling them to comply with data protection legal requirements on workplaces.

2. c) *Biometric identification*

A client in her submission requested the Authority to deliver an official statement whether the data processing of a school could be lawful where the education institution intends to install a biometric identification system at entry points.

Considering the relevant national and EU regulations the client was advised as follow.

Fingerprints of a natural person qualify as personal data and taking of fingerprints qualify as data processing. Both the relevant national legislation and the EU Data Protection Directive stipulates fundamental legal principles which should also be regarded in data processing activities. These include e.g. the principle of proportionality (et al.).

The Authority found that a biometrics system – aimed at taking fingerprints of pupils upon entering the school – for the purpose of personal security and the protection of property does not meet the requirements of proportionality. Better identification, instead, could be secured by any other – more harmless and less intrusive to privacy – ways.

Consequently the introduction of such an entry system would jeopardize the privacy rights of data subjects concerned.

2. d) *Cloud computing*

A political association lodged a petition with the Authority and requested its statement on the lawfulness of the association's data processing activity. The association (hereafter: data controller) indicated its wish to process personal data of their supporters by means of cloud computing technology. They added they plan to choose a cloud computing service provider of which parent company is registered in the U.S. whilst it has a subsidiary in Ireland. The service provider in question is said to be on the safe harbour list published by the U.S. Department of Commerce.

The Authority found that the sensitive nature of personal data of supporters of a politically active association significantly increases the security concerns, indeed. Therefore the Authority opposed to the transfer of such personal data to the „cloud".

2. e) *Hacking of internet site of Capital Mineral Water and Beverage Co. Ltd.*

In October 2012 a Turkish hacker group was said to have compromised the internet promotion site of the above company. As a result more than 50.000 personal data (name, email address, date of birth etc.) were stolen. On this occasion our Authority delivered an announcement in which we questioned why the personal data of consumers had been made accessible online or why these personal data had not been encrypted. Simultaneously we called for higher consideration of data security measures to be introduced and applied in order to avoid similar eventual data breaches.

In this matter a data protection administrative procedure is still in progress.

2. f) *Financial penalty to an internet publishing company*

We have received a complaint from an individual stating that s/he has been getting unsolicited marketing emails from a company to which s/he has not consented to as well as the company failed to terminate the service and to delete the contact details of the complainant despite his/her continuous requests to do so.

As a result of an investigation and afterwards a data protection administrative procedure the Authority imposed a financial penalty of 3 million HUF. This huge amount had been decided due to the following aggravating requirements: the wide scope of persons affected by the unlawful processing; the high number of minors concerned; the severity of the infringement as well as the extraordinary duration of the unlawful situation. Extenuating circumstances had also been taken into consideration as follow: the finalization of a new privacy policy; making it accessible on the website; the reporting of amendments into the data protection registry. This willingness of the controller to cooperate with the Authority was demonstrated by the velocity by which the controller performed the necessary modifications that were made right after the data protection procedure had been initiated.

2. f) *The Századvég case*

The Ministry of National Development turned to the Authority inquiring whether analyses and studies created by business contracts concluded with the Századvég Foundation, Századvég Economic Research Plc. as well as Strategopolis Strategic Analytics and Communication Consulting Co Ltd. can be subject to disclosure. According to the Ministry these papers were governmental preparatory documents. Our Authority found that the documents in question had been prepared from public funds and to public authorities that's why they qualify as being data of public interest and data public on grounds of public interest (except personal data possibly contained therein).
The Authority emphasized that the restriction of disclosure over preparatory documents in a decision-making process must not lead to the exclusion of transparency. (NAIH-4442/2012/V)
The case ended up with a judicial procedure where the court ruled in favour of disclosure of the documents in question at first instance.

2. h) *"Protection of children" project*

The NAIH, in close cooperation with the Parliamentary Commissioner for Fundamental Rights, elaborated a project leaflet with the purpose of calling the attention of children to the safe and conscious internet surfing, the threats of web communication, the contents that can be harmful for their spiritual and mental development as well as how to cope with them. This leaflet is divided into five sections:

1. basic rights of children and human rights organizations dealing with the enforcement of childrens' rights;
2. major risks posed by the internet and the techniques to realize them;
3. best practices from abroad
4. institutions in Hungary empowered to protect and support minors in case of abuses
5. guidance to conscious and safe internet use

Composed by: dr. Balázs Mayer

Memorandum of Understanding with US Federal Trade Commission

In June 2013, the Data Protection Commissioner signed a Memorandum of Understanding with the US Federal Trade Commission. The aim of the MOU is to support increased cooperation and communication between the two agencies in their efforts to ensure protection of consumer privacy and data protection rights.

Audit of Facebook Ireland

On 21 September 2012 the Office of the Data Protection Commissioner published the outcome of its Review of Facebook Ireland's (FB-I) implementation of recommendations made in the Office's Audit of the social networking site in December 2011. The 2011 Audit Report was a comprehensive assessment of Facebook Ireland's compliance with Irish Data Protection law and by extension EU law in this area. Facebook Ireland's delivery on its commitments in that Report was evaluated throughout the first half of 2012 and formally on-site in Facebook's European HQ in Dublin from 2-3 May and 10-13 July 2012.

The Review found that the great majority of the recommendations have been fully implemented to the satisfaction of the Office of the Data Protection Commissioner, particularly in the following areas:

- The provision of better transparency for the user in how their data is handled,
- The provision of increased user control over settings,
- The implementation of clear retention periods for the deletion of personal data or an enhanced ability for the user to delete items,
- The enhancement of the user's right to have ready access to their personal data and the capacity of FB-I to ensure rigorous assessment of compliance with Irish and EU data protection requirements.

Several recommendations which were not implemented by FB-I in 2012 have since been implemented during the course of 2013. These have been examined and signed off by the Office of the Data Protection Commissioner.

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

The review report is available on the Data Protection Commissioner's website:
http://dataprotection.ie/docs/Facebook_Audit_Review_Report/1232.htm

Major developments in the data protection field – ITALY

Legal persons An amendment introduced via decree [2] to the Data Protection Code (Section 4, Legislative Decree no. 196 of 30 June 2003

(http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003 April2013.pdf)

excluded legal persons from the definition of "personal data" – whereby a personal data is "any information relating to a natural person" only. This means that the DP Code currently does not apply to the processing of personal data relating to legal persons (including associations, foundations, committees, etc.). However, the DPA issued a detailed opinion (published ultimately in October 2012) to clarify that this is to be construed not to exclude legal persons to the extent they are "contracting party" to a publicly available electronic communications service as per the definitions contained in the DP Code in pursuance of the e-privacy directive (Section 4(2)f.).

Data breach New provisions were introduced by legislative decree no. 69 dated 28 May 2012 (Section 1(1)b) which implemented the EU regulatory framework for electronic communications provided for by Directive 2009/140/EC.

In particular, decree no. 69/2012 introduced the definition of "personal data breach" (Section 4 (3)g bis of the DPCode) and a new provision (Section 32 bis of the DPCode) which sets forth the obligation for the provider of publicly available electronic communications services, without delay, to notify a personal data breach to the Garante. The contracting party or the individual must also be notified when the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual.

Penalties against providers of publicly available electronic communications devices were also introduced in respect of non compliance with the data breach obligations (Section 173 bis of the DPCode). The Italian DPA on 4 April 2013 adopted a decision regarding the "Implementing Measures with Regard to the Notification of Personal Data Breaches" (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2414592).

The decree 69/2012 also amended the DPCode provisions regarding the information collected with regard to contracting parties or users, in particular in respect of cookies (Section 122 of the DPCode). The new regime, which confirms the opt in system, provides for simplified modalities for the information to be given to the data subject and for the expression of his/her consent.

Security Measures The decree no 5, dated 9 February 2012, as converted, with amendments, into Act no. 35 dated 4 April 2012 repealed the obligation for data controllers to submit the so-

[2] Decree no. 201 dated 6 December 2011 subsequently converted, with amendments, into Act no. 214 dated 22 December 2011

called “Security Policy Document” (Documento programmatico per la sicurezza, DPS) to the DPA. It should be recalled that all the other security measures continue to be fully applicable.

The same decree repealed the provision of the DPCode which provided for the power of the Garante, by own decision, to determine simplified arrangements to implement security measures in respect of data processing that is carried out for standard administrative and accounting purposes (in particular by SMEs, self-employed professionals, and handicrafts).

Judicial data

The decree no. 5/2012 also modified the regime for processing of judicial data as provided for by Section 21 of the DPCode. The new provisions allow the processing of judicial data if it is performed in pursuance of memorandums of understanding for preventing and countering organised crime that are entered into with the Ministry for Home Affairs and/or peripheral offices, with the prior opinion of the Garante, which memorandums shall specify the categories of processed data and the processing operations to be performed.

LATVIA / LETTONIE

ANNUAL REPORT 2012

A: A summary of the activity and news:

Within the year 2012 the draft of amendments to the Personal Data Protection Law has been elaborated. Mainly the amendments relate to the following issues:

- Clarification of the definition of the controller, including the definition of joint-controller, by determining the rights and duties, as well as the shared responsibility.
- Determination of several more exemptions from notification.
- Specified requirements regarding data transfers to the third countries that do not ensure such data protection level as it is in Latvia.
- Requirement for the state and local government institutions to implement evaluation of effectiveness of personal data protection.
- Determination of the rights of Data State Inspectorate to determine a certain time frame when the information should be submitted to Data State Inspectorate in order to carry out its functions.

There have been also amendments elaborated regarding the Schengen Information System. Data State Inspectorate of Latvia in cooperation with the Ministry of Justice has issued an opinion that it should be revaluated and reconsidered if all the institutions need the access to SIS and for which purposes.

At the national level Data State Inspectorate of Latvia provided its opinion regarding the different legal acts and policy initiatives, listing the main ones bellow:

1) Draft Law on Credit Bureau;

2) Draft Law on Debt Retrieval;

3) Draft Law on the Electronic Identification.

In October 2012 Latvia had the Schengen evaluation regarding data protection and thus it was the priority of the office (several control activities were carried out, as well as information materials elaborated).

Considering the complaints received in 2011 and 2012, Data State Inspectorate of Latvia has identified the following issues where majority of the complaints were received:

1) Personal data processing within the debt collection process;
2) Controller has not provided the necessary information to the data subject;
3) Publishing of personal data on the internet.

There have been 10 seminars organised, as well as 3 exams for the data protection officers. 12 persons have obtained the status of data protection officers.

Key topics where advice was requested from public authority

Data State Inspectorate does not have any statistics available on the requests for advice submitted by public authorities. However Data State Inspectorate daily receives calls from different public authorities on variety of issues related to personal data processing – starting with

the necessity to notify the personal data processing, data subject's access rights and following more complicated questions which require in-depth analysis in order to find out the best solution regarding personal data protection (for instance, there have been relatively many questions raised by the public and private sector regarding the data processing aspects within the labour relations and data security issues therefore Data State Inspectorate of Latvia in 2013 will elaborate recommendations on these issues).

Information on awareness raising activity

Data State Inspectorate has organised several seminars on the issues for personal data protection, for different target audiences – for instance, educational establishments, local government institutions, bank and finance sector representatives, medical staff, etc. Data State Inspectorate provides seminars which are open for all the persons interested.

There are at least 4 media requests each week regarding different data protection issues. Attention has been also paid by media to the issues considered at the Article 29 Working Party, as well as to the outcome of the joint Baltic countries' investigations regarding personal data processing.

Since there were several control activities carried out regarding the loyalty cards, there was media support on this issue by motivating people to think about their personal data as value and to evaluate more careful which are the cases when personal data should not be submitted to the persons/ companies that request it.

Key figures related to DP

Organisation	**Data State Inspectorate of Latvia (Datu valsts inspekcija)**
Chair and/or College	Director – Signe Plūmiņa
Budget 2012	266 907 LVL (aprox. 370 457 EUR)
Staff	19 (including the administrative and maintenance staff)
General Activity	
Decisions, opinions, recommendations	Regarding the statistics on decisions, opinions – N/A. Regarding the recommendation – no recommendation elaborated in 2012; two recommendations foreseen in 2013
Notifications	352 (including the notifications on amendments to personal data processing)
Prior checks	234; focused on the risk areas (determined for each year) such as processing of sensitive data, biometric data processing (including video surveillance), and personal data transfer to the third countries.

Requests from data subjects	N/A
Complaints from data subjects	Total number of investigations – 496 (80% of investigations were carried out due to the complaints received). 4 complaints from data subjects from the third countries regarding their personal data processing within SIS. 11 complaints regarding SPAM (11 investigation carried out thereof).
Advices requested by parliament or government	Regarding several legal acts, for instance, Draft Law on Credit Bureau, Draft Law on Debt Retrieval, Amendments to the Schengen Information System Operation Law.
Other relevant general activity information	During the telephone consultation times the main questions asked by the callers: 1. Is certain information considerable as personal data? 2. When, who and where can carry out video surveillance? 3. How to fight against unlawful personal data processing in the internet? 4. Personal data processing within the debt-collection process. 5. How can data subjects exercise their rights for data protection more effectively?
Inspection activities	
Inspections, investigations	Mostly people who contacted Data State Inspectorate of Latvia have indicated on possible breach of Personal Data Protection Law in the following areas (similarly as in previous year): 1) personal data processing on the internet (also in cases when the controller has not foreseen appropriate technical means for data protection); 2) personal data processing related to the debt collection and setting up the credit history; 3) identity theft – when personal data of another person are provided thus unlawful personal data processing carried out (many cases regarding wrong personal data submitted to State or Local Government Police regarding several administrative violations); 4) data processing carried out by house maintenance

	companies; 5) video surveillance.
Sanction activities	
Sanctions	The sanctions of Data State Inspectorate are provided within the Latvian Administrative Violations Code.
Penalties	There have been fines applied for 18 910 LVL (~26 119 EUR). The biggest fine was LVL 2000 (~2762 EUR) that was applied to a debt collecting company for illegal personal data processing and for not providing the information to a data subject. Two fines were applied regarding the personal data processing within SIS.
DPOs	
Figures on DPOs	12 Data protection officers registered.

B. Information on case law

In 2012 the number of those cases increased where Personal Data Protection Law has been violated and the sanctions for such violations are foreseen with the Criminal Law, thus these cases were forwarded to the office of prosecutor general. Also the number of those cases has increased where there was a necessity to cooperate with DPAs of other EU countries in order to carry out the investigation.

Part IV Contacts

Data State Inspectorate
website: www.dvi.gov.lv

LIECHTENSTEIN

Country report
Principality of Liechtenstein

Legal developments:

A revision of the Code of Criminal Procedure and of the Data Protection Act, mentioned in last year's report, entered into force in October 2012. This revision was necessary following the Framework Decision on Data Protection in the Third Pillar. With the revision of the Data Protection Act, the regulation on information to be given to the data subject (Article 5) and to notify data files by companies (Article 15) were amended to be more in line with the general Data Protection Directive 95/46/EC.

Other developments:

Guidelines were published on the notion of, and difference between, anonymity and pseudonymisation. It is hoped that these guidelines will be helpful in practice, in particular, considering developments, such as "big data".

Furthermore, a sample for privacy notices to be used for internet sites were made accessible to the public.

In the framework of data retention, inspections were conducted with the major providers.

Awareness-raising activities

At the occasion of the European Data Protection Day, a public event was organized together with the University of Liechtenstein on the subject *"Do I really have nothing to hide? About the value of privacy at the age of the Internet.*

The Data Protection Act celebrated its 10th anniversary in 2012. For this reason, the Data Protection Office commissioned a survey of the public about the status of awareness on the basis of the 2008 Eurobarometer "Data Protection in the European Union – Citizens' perceptions – Analytical Report". The results showed that, amongst others, more awareness-raising activities are needed. This, however, is not only the task of the data protection office. Co-operation with other bodies should lead to fruitful synergies.

For more information, please consult the Internet site of the Data Protection Office on www.dss.llv.li (in German only).

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

1. Recent National Developments – legal framework

1.1. No changes of the Law on Legal Protection of Personal Data of the Republic of Lithuania (Official Gazette, 1996, No 63-1479; 2008, No 22-804) since year 1211, when the last changes have been made.

1.2. *The Law on Electronic Communications of the Republic of Lithuania*
Changes of the Law on Electronic Communications of the Republic of Lithuania (Official Gazette, 2004, No 69-2382; 2008, Nr. 87-3468, No 131-5037, Nr. 137-5383) have been made due to obligations of electronic communications services operators to provide an information to law enforcement bodies. Article 77 paragraph 1, 3, 4, 5, 6 and 7 specify that market players shall provide an information necessary for crime prevention, investigation purposes and in other cases laid down by laws, to an institution of criminal investigations free of charge by means of electronic communications without delay and in the manner laid down in laws. New version of that article establishes that data security measures should be implemented by law enforcement bodies, all other entities and agencies which are entitled to share above mentioned information and authorizes the Government to set an order of that information sharing.
The State Data Protection Inspectorate (hereinafter – SDPI) is empowered to supervise data processing performed by operators and other market players. SDPI is empowered to check the procedures also number of enquiries and applications, replies to them as well as legal background for any transfer of personal data.

1.3. *Draft on the amendment and supplement of the Law on Electronic Communications of the Republic of Lithuania*
Taking into account entering into force Regulation No 611/2013 of the European Parliament and the Council of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (OJ 2013, L 173/2) prepared the Draft of the of the amendment and supplement of the Law on Electronic Communications. The Draft is given to Seimas (the Parliament). The possibility to notify about personal data braches by electronic means via SDPI website is implemented, the address is https://www.ada.lt/go.php/lit/6-Pranesimas-apie-asmens-duomenu-saugumo-pazeidima/4/20 .

2. Major case law

2*.1. Use of a personal identification number for the purpose of direct marketing and definition of a consent*
The SDPI after handling of a complaint issued the order to the data controller that personal identification number should not be collected as obligatory attribute if a contract to which the data subject is a party is being concluded by filling a standard form when these data are being collected for a purpose of direct marketing. SDPI also stated that the data controller must provide a clear, free-of-charge and easily realisable possibility for the data subject to give or refuse giving his consent for the processing of his/her personal data for the purposes of direct marketing. The data controller appealed the decision of the SDPI on the ground that the consent of the data subject to use above mentioned number has been given. Data controller also gave a reasons that data subject has right to write in free form about withdrawal of the consent if it is already done.

The Court of first instance did not satisfy an appeal and stated that the consent to use personal identification number for the purpose of direct marketing cannot be treated as given freely by a data subject if that is confirmed only by signing the agreement for services provision and left the order of the SDPI without changes. The data controller appealed this decision to the Supreme Administrative Court of Lithuania but the Court did not change the decision of the court of first instance by deciding that a clear, free-of-charge and easily realisable possibility for the data subject to give or refuse giving his consent for the processing of his/her personal data for the purposes of direct marketing has not been provided. The consent to use personal identification number for the purpose of direct marketing could not be treated in the same manner as for the conclusion of the contract to which the data subject is party.

2.2. Disclosure of personal data

The SDPI received a complaint that administrator of taxes had a speech on TV and disclosed personal data of a person who has been suspected in tax evasion.

The SDPI after handling of a complaint issued the order to the data controller that personal data should not be disclosed publicly without any legal background because Article 38 Paragraph 1 of the Law on Administration of Taxes of the Republic of Lithuania ((Official Gazette, 2004, No 63-2243) states that information about tax payer is confidential and should be used only for legitimate purposes. The data controller appealed the decision of the SDPI on the ground that the right to know is very important for the society and the disclosure of information about payment of taxes to the public shall be understood as transparency and may be lawfully used by the public.

The decision of the first instance Court satisfied the appeal of the tax administrator. The data controller appealed this decision to the Supreme Administrative Court of Lithuania and the Court of changed the decision of the court of first instance by deciding that an information related to violations of the Law on Administration of Taxes should be kept confidential while being of an offence is not proven and there is no Court decision that the tax payer is guilty. Court also stated that the administrator of taxes is competent institution for the protection of the interests of the State but also has an obligation strictly observe the law and do not infringe rights of the tax payers.

3. Preventive activity

3.1. *Consultations*

Seeking better understanding requirements of data protection laws the SDPI provides consultations by telephone, by e-mail, by mail and organizing meetings of data controllers. 4 public consultations have been published in year 2012, also delivered 915 consultations to data subjects and 2500 – to data controllers.

3.2. *Inspections on the SDPI initiative*

SDPI made 45 planned investigations on its' initiative in year 2012 in total. Inspections were conducted in 26 companies providing e-shopping services in order to determine whether the aforementioned companies, processing data of the customers ensures proper implementation of data subject's rights, legitimacy of data retention and right of access. Any violations of the laws on data protection were not found only in 3 companies.

.

3.3. In year 2012 Estonian, Latvian and Lithuanian data protection supervisory authorities conducted coordinated inspections in frame of Baltic States cooperation. Investigations in hotels belonging to the Radisson Blue international network were carried out in all three countries in year 2012. The aim of the investigations was to check legality of the hotel guests personal data processing for accommodation purpose. During investigations several incompatibilities to personal data protection requirements were established and orders to the hotels given.

4. Public awareness

4.1. In aim to raise data protection awareness European Data Protection Day was celebrated on 30th January 2012. Press conference at the Seimas of the Republic of Lithuania on Data Protection Day "Data protection and modern technologies" were organised for general public. Special attention SDPI pays to the target groups of young people. On 7th February 2012 the Data Protection Day was organised for schoolchildren of the Vilnius Lyceum. Representatives of the SDPI and schoolchildren spoke about threats to personal data security and possible damages while using modern technologies.

4.2. Training on data protection has been provided by SDPI during training courses organized by Ministry Foreign Affairs on 12.03.12 for the consuls and other employees of the Ministry. During this event SDPI noticed that it is shortage of information dedicated for travelers SDPI prepared the memo for people crossing the Schengen borders, which was published on the website of the Ministry of Foreign Affairs and the leaflet in three broadly used languages in Lithuania (Lithuanian, Russian and English) on data subject rights, which was disseminated at the police offices and the border crossings points.

4.3. On 13.09.2012 SDPI organized one day workshop for the Ministry of Foreign Affairs, the Ministry of Interior and other law enforcement bodies which staff is processing personal data by the Schengen acquis. Representatives of the SDPI delivered reports and held a discussion.

4.4. The SDPI together with a public relations company on 19.05.2012 organized a conference "Employees personal data processing and the disclosure of data to third parties – topic issues and problems". The conference was focused on the broad guidelines of data processing issues important for private companies, governmental institutions and organizations, managers, lawyers, professionals responsible for employees' personal data processing. The event was dedicated to the 15th anniversary of the SDPI.

MONACO

Les développements majeurs survenus dans le domaine de la protection des données à Monaco depuis juin 2012, date de la dernière session plénière

- Le groupe de travail de l'article 29 de l'Union Européenne a, par avis adopté le 19 juillet 2012, émis un avis favorable sur la demande de protection adéquate introduite par la Principauté.

- Les normes simplifiées suivantes ont été adoptées:

- Arrêté Ministériel n° 2012-575 du 4 octobre 2012 relatif aux modalités de déclaration simplifiée des traitements informatisés d'informations nominatives relatifs à la « gestion des fonds sociaux».

- Arrêté Ministériel n° 2012-359 du 21 juin 2012 relatif aux modalités de déclaration simplifiée de conformité des traitements automatisés d'informations nominatives portant sur la « gestion des services de téléphonie fixe et mobile sur les lieux de travail ».

- Arrêté Ministériel n°2012-575 du 4 octobre 2012 relatif aux modalités de déclaration simplifiée des traitements automatisés d'informations nominatives relatifs à la gestion des fonds sociaux.

- Arrêté Ministériel n° 2013-200 du 11 avril 2013 relatif aux modalités de déclaration simplifiée de conformité des traitements automatisés d'informations nominatives relatifs à la gestion des dossiers patients des professionnels de santé exerçant à titre libéral

- La CCIN a émis les recommandations suivantes :
- n° 2012-147 du 22 octobre 2012 portant recommandation sur les délais de conservation des informations nominatives se rapportant à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

- n° 2012-118 du 16 juillet 2012 portant recommandation sur les dispositifs d'enregistrement des conversations téléphoniques mis en œuvre sur le lieu de travail par les établissements bancaires et assimilés ;

- n° 2012-119 du 16 juillet 2012 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité "*gestion de la messagerie professionnelle*" utilisés à des fins de contrôle de l'activité des employés.

NORWAY / NORVÈGE

Developments in the Norwegian legislation on protection of personal data

To: T-PD

From: The Norwegian Ministry of Justice and Public Security

Date: 28.06.2013

1. INTRODUCTION

In the following we will present an update on the major legal developments in Norway concerning personal data protection since the 29th meeting of the T-PD.

2. NEW LEGISLATION ON PERSONAL DATA PROTECTION IN THE POLICE SECTOR

In 2010 a new act on the processing of personal data in the police sector was adopted by the Norwegian Parliament. The act is not yet put into force. The aim of the new act is to ensure the necessary protection of personal data while providing the police with the tools necessary to solve their tasks in an effective manner.

Provisions on secrecy and transfers of personal data constitute an essential part of the proposal. The new act gathers the provisions on secrecy and transfers in one act, in order to simplify and make the provisions more user friendly. In addition the provisions on DNA-registers and fingerprints are moved from the procedural act to the new act on processing of personal data in the police sector. This is meant to create a clearer division between rules on processing of personal data and rules governing purely procedural aspects.

The act also contains new rules on the issuing of criminal record certificates. For instance the act contains specific rules concerning in what cases acts committed by people of young age should be listed on a criminal record certificate.

3. NEW DECISIONS FROM THE PRIVACY APPEALS BOARD

In a decision of 19th June 2013 the Privacy Appeals Board upheld the Norwegian supervisory authorities' decision ordering the Norwegian Institute of Public Health to delete personal data which has been stored without the necessary legal basis for continued processing. The case concerned, amongst other issues, questions relating to DNA-samples which the institute analysed on behalf of the police. The DNA-samples were kept after the analysis ordered by the police was carried out, even if the institute had no legal basis for such storage.

PORTUGAL

As requested, please find below the information regarding the Portuguese legislative developments connected with data protection that took place since 30th November 2012, which was the date of our last Plenary.

No changes occurred to domestic data protection legislation.

The following legal instruments have their own specific provisions about personal data.

- Decree-Law nr. 14/2013, of 28th January, regarding the citizen's individual tax payer number, introduced some changes regarding the citizen's identification as tax payers. The changes are related to the on-line access to that data.

- Law nr. 40/2013, of the 25 July, that approves the rules of organization and functioning of the Council for the monitoring of databases of ADN profiles. This public authority whose members are designated by the Parliament, work in strict connection with the Portuguese personal data protection authority.

- Law n. 527/2013, of 25 July, makes some changes to the 2009 Law concerning fighting against violence, racism, xenophobia and intolerance in sport events in order to improve the security on those events. Personal data of concerned persons, namely spectators, mainly if a previous administrative or criminal sanction was imposed in any EU country is collected and processed.

ROMANIA / ROUMANIE

Romania - ANSPDCP

Video surveillance

In view of the frequent use of video surveillance systems, as well as of the fact that the illegitimate, inadequate or excessive use of such means may infringe upon the fundamental rights and liberties of natural persons, the National Supervisory Authority for Personal Data Processing issued Decision no. 52/2012 on this particular type of personal data processing.

The Decision provides that video surveillance means may be used in open places and areas or similar public spaces, inclusively on public access ways on public or private domain, within the conditions provided by law. Video surveillance cameras must be installed in visible places – the use of hidden video surveillance means is prohibited, except for the cases provided by law. The Decision's provisions also forbid the installation of video surveillance means in spaces which particularly require observance of the individuals' privacy such as fitting rooms, dressing rooms, shower stalls, toilets and other similar places.

As regards the information of data subjects, one of the obligations imposed on data controllers is to signal the use of a video surveillance system through the use of an indicative and representative image, with sufficient visibility and positioned at a reasonable distance from the places in which the video surveillance equipment is installed.

The storage period of the data obtained through the use of video surveillance means must be proportionate with the processing's purpose, but not exceed 30 days, except for the cases expressly mentioned by law or thoroughly justified.

One recent example of the enforcement of the provisions of Decision 52/2012 is that of the negative notice issued in August this year by the National Supervisory Authority for Personal Data Processing following a request submitted by a city hall to use video surveillance means for its own staff members, inside the offices where they carried out their activities. The negative notice referred to the need to ensure an efficient protection of the employees' right to private life; a finding was also made on the fact that the processing is excessive with regard to the intended purpose and infringes the employees' private life.

Processing of personal data of pre- paid card users

The National Supervisory Authority for Personal Data Processing has given a negative opinion with regard to a legislative proposal on the collection and storage of the data necessary for the identification of customers of electronic communication services provided via pre-paid cards. The provisions of this legislative proposal came into contradiction with the principles established by Council of Europe's Convention 108, as well as with the provisions of Directives 95/46/EC, 2006/24/EC and Directive 2009/136/EC on universal service and users' rights relating to electronic communications networks and services.

Moreover, the legislative proposal infringed on the individuals' right to private life (established under Article 26 of Romania' Constitution, as republished). The processing of the Personal Identification Number (CNP) ma be carried out in accordance with the conditions provided by article 8 of Law no. 677/2001 and these of Decision 132/2011; however, as the legislative proposal was drafted it brought serious infringements to the principles of proportionality and storage of data as provided by Directive 95/46/EC and Law no. 677/2001.

By establishing the obligation to communicate the identification data upon the data subjects that had already acquired a service of any type from the providers of the electronic communication service, prior to the entry into force of the proposed act, the supervisory authority considered that it infringes on the principle of non-retroactive laws, established under article 15 paragraph (2) of Romania's Constitution.

The legislative proposal mentioned above also brought infringements upon the consumers' right to make decisions with regard to acquiring pre-paid communication services, as, by imposing the obligation for identification, that might influence the consumer's option with regard to acquiring the service or not.

Sanction imposed on RATB – Bucharest's City Transport Co.

In view of the risks posed on the private life of a significant number of persons, the National Supervisory Authority for Personal Data Processing has imposed a contraventional fine on the RATB – Bucharest's City Transport Co. for making copies of the identification documents of pupils and students that applied for a transport pass with subsidised price.

Following the investigation it was ascertained that the data controller scanned and stored copies of identification documents, as well as other documents, that contained the applicants' personal identification number, thus infringing the provisions of article 8 of Law no. 677/2001. Moreover, making copies of identification documents containing the personal identification number is forbidden, according to the provisions of article 6 of ANSPDCP's Decision no. 131/2011, except for the cases in which there is an express legal provision, the data subject's contain is obtained or there is an approval of the supervisory authority.

ANSPDCP decided that the RATB stop maintaining the copies of the respective documents and delete the data base it had established, within 10 days of ANSPDCP's decision.

Appointment of ANSPDCP's new president

By Romania's Senate Decision no. 48 of 26th June 2013 Mrs. Ancuţa Gianina Opre was appointed as president of the National Supervisory Authority for Personal Data Processing.

Mrs. Ancuţa Gianina Opre currently also carries out her activities as an associate professor within the Faculty of Legal and Administrative Sciences of the Christian University "Dimitrie Cantemir" in Bucharest. Mrs. Opre has a professional experience of over 10 years in the field of law and has previously (2009) occupied the position of president of the National Authority for Property Restitution.

SERBIA / SERBIE

Report on the latest developments in the field of data protection in Serbia Since June 2012

1. **Legal Framework**

Since June 2012 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 electronic communication and access to retained data confirming, once again, that a court order was need for any access to electronic communication data. 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 Military Intelligence Agency and Military Security Agency.

2. **Cases**

There have been no significant changes.

Number of cases pertaining to personal data protection is rising continuously. Average number of cases received per month is around 100. Exceptionally in 2013, in March, April and June Commissioner received 174, 227 and 322 cases respectively.

3. **Commissioner's Office**

In August 2013 the Commissioner was allocated new premises which are expected to be functional in late September 2013/early October 2013, following the refurbishment.

Note: the lack of adequate premises has been the most significant obstacle for the overall work of the Commissioner and the hiring of new staff, noted also in several EU Progress Reports.

Current total number of staff is 46 (according to the approved internal organisation total staff number is 94 – Commissioner is competent for freedom of information and personal data protection).

Upon the relocation to the new premises the recruitment of new staff is expected to start.

4. **Data Protection Day, 28 January 2013**

Press conference.

5. **Projects and important activities**

Hosting the 15th Meeting of the Central and Eastern Europe Data Protection Authorities: on 10-12 April 2013, the Commissioner was a host to the 15th CEEDPA, the annual meeting of the representatives of the Central and Eastern Europe Data Protection Authorities. Executives or representatives of the competent authorities from 14 countries of Central and Eastern European region participated in the meeting: Albania, Bosnia and Herzegovina, Bulgaria, Hungary, Macedonia, Poland, Russia, Slovakia, Slovenia, Serbia, Ukraine, Croatia, Montenegro and the Czech Republic. The special focus was on: data security, data processing in the field of employment, as well as the independence of the competent authorities for the personal data protection and the challenges.

Capacity building of the Office of the Commissioner commenced in April 2012 and finalised in December 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.

SLOVAK REPUBLIC / REPUBLIQUE SLOVAQE

Based on your email from 19 June 2013 we would like to inform you that by the July 1st 2013 a new Act No. 122/2013 Coll. on personal data protection and about amendment of other acts (hereinafter referred to as “new PDP Act”) which invalidates standing act No. 428/2002 Coll. (hereinafter referred to as “old PDP Act”) entered into force. Objective of the changing of the old PDP Act was to transpose the Directive of The European Parliament and The European Council 95/46/EC, implement conclusions and recommendations of Schengen evaluation in the Slovak Republic in the personal data protection area and law analysis from application practice point of view.

The new PDP Act brings mainly a better outline to legal area, definition and specification of particular processes. It specifies definitions of some terms, which the law operates with and the familiarization of which is needed before the personal data processing starts. The new PDP Act removes misinterpretations of some of the basic provisions of the old PDP Act, which caused frequent need for clarification in application practice. For instance, application practice brought the need to increase qualification of data protection officers (hereinafter referred to as “DPO”) and therefore The Office for Personal Data Protection of the Slovak Republic (hereinafter referred to as “Office”) came to a decision to assume more restrictive requirements for exercising this function, mainly by passing an examination at the Office.

Experience also exposed the need to ensure that controllers and processors pay increased attention to personal data protection and improve security of data being processed as well as qualification of DPOs. The most important changes compared to the old PDP Act are as following:

The new PDP Act

- specifies the definitions of basic terms,
- brings better specification of controller’s and processor´s status as well as relations between them,
- specifies obligation for controllers which are not established in the EU to appoint a representative that is located in the territory of the Slovak Republic and requirements for this institute,
- extends processing of personal data without the consent of data subject, namely in the case where such processing is performed pursuant to directly applicable acts of the EU or international convention which is binding for the Slovak Republic,
- takes into account technological development and gives permission to prove consent regarding to the national legislation – consent given in electronic form with secured signature pursuant to special act,
- newly regulates requirements for the processing of biometric data
- extends the time-limit for storage of recordings provided by monitoring of premises accessible to the public from 7 to 15 days,
- introduces obligation for controller in case of providing inaccurate personal data to third parties to notify them of this matter, as well as obligations of third parties,
- clearly define the scope and documentation of security measures,
- specifies the institute of the entitled person (person entering in contact with personal data at the controller),
- newly regulates requirements for appointing of DPO (the new PDP Act sets mandatory passing of an examination in order to exercise this function at the Office),
- strengthens the mechanisms for protection of data subject´s rights,

- changes conditions for cross-border flows of personal data to third countries which do not ensure an adequate level of protection,
- specifies conditions of registration and introduces registration fee for filing systems,
- specifies further the position of the Office and extends its scope of competences in the area of personal data protection (e.g. to guide methodically the controller and processor, the competency to approve binding corporate rules, execution of DPO exams and obligation to notify the Office in case of the change in DPO assignment etc.),
- redefines the performance of control of compliance with personal data protection,
- sets out new procedural rules in case of violation of the law,
- introduces compulsory infliction of a fine in case of violation of the law, i.e. the Office is always obliged to impose a fine for violation of the law.

Stanislav Ďurina
Head of the International Relations Department
Office for Personal Data Protection of the Slovak Republic

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

REPUBLIC OF MACEDONIA

DIRECTORATE FOR PERSONAL DATA PROTECTION
www.privacy.mk

Developments in the data protection field in Republic of Macedonia
(July 2012 – August 2013)

Inspection

Main competence of the Directorate is supervision over the legality of the activities taken in the processing of personal data and their protection on the territory of the Republic of Macedonia. The performance of inspection in the Data Protection Authority is organized in a particular sector - Sector for inspecting with two departments.

In the frames of the Software for the inspection supervision SIN and the Strategic plan of the Data Protection Authority, the inspections are planed on an annual basis, in different areas, with a program customed made at the end of the current year for the following year, and it is implemented through monthly plans for inspection with specified controllers, the collections being inspected and the date of commencement of inspection supervisions. The Annual Program for 2012 and Monthly Plans for inspection (January-December 2012) are published on the website www.privacy.mk.

The execution of the regular inspections supervision is carried out in a clearly defined bylaws and procedures during the inspection. Inspectors in the course of regular inspections carried out educate the controllers and processors of personal data protection law, puting the preventive role as a priority in repressive actions of inspectors, as well.

Namely, during the 2012 a total of 368 inspections are performed out of which 273 are regular inspections, 95 incidental incidental inspections. 28 Cases from 2011 were transferred and all were complete during 2012. In the first half of the 2013, 220 inspection supervisions were performed.

The inspectors of the Data Protection Authority permanently were included in capacity building trainings as well as performed work as presenters and trainers in many trainings for controllers, presenters and organizers of a numerous conferences and projects in the area they work. At the same time conditions were enabled for the work of the inspectors meaning their direct education and equipping with the latest IT technology. After acquired ISO 27 001 in 2011, in 2012 the inspectors have gained ISO 27005 Risk Management cerificate. With these certifications, inspectors have increased their capacity for supervision of controllers and processors including risk management in a complex IT infrastructure.

Main priority in performing inspection supervision in the first half of the 2013 was the inspection over protection of personal data from the public prosecutors offices in the Republic of Macedonia. The Report for the protection of the personal data in the Public Prosecutors offices

will be submitted to the EUROJUST till the end of 2013, according to the Agreement for cooperation between the Republic of Macedonia and EUROJUST.

Public awareness rising

Public awareness rising and informing the citizens about their right of personal data protection and privacy remains the key imperative of the work of the Data Protection Authority. Data Protection Authority focused its work on affirmation of the right of personal data protection among the citizens and education of the controllers.

Media	Number of appearances
Printed media	52
TV	53
Radio	27
Web media	42
Total	**174**

International cooperation

- Signed Agreed Guidelines for cooperation between the Data Protection Authority and the Data Protection Officer of EUROJUST

Continuous cooperation with EUROJUST – received an approval for participation of the Data Protection Authority as an observer of the working meetings of the Joint Supervisory Body of EUROJUST, on issues of interest to the Directorate in accordance with the signed Agreed Guidelines for cooperation between the Data Protection Authority and the Data Protection Officer of EUROJUST. A step forward was made recently towards the implementation of the provisions of the signed Agreement for cooperation between the Republic of Macedonia and EUROJUST ("Official Gazette of the Republic of Macedonia nr. 51/09) and the Agreed Guidelines between DPO EUROJUST and the Data Protection Authority.

The collaboration with Data Protection Office in EUROPOL was in this period enhanced in relation to the implementation of the provisions of the signed Agreement on operational and strategic cooperation between RM and EUROPOL and competencies in accordance with the Agreement ("Official Gazette of the Republic of Macedonia nr. 172/11).

International Workshop - "Balkan Conference of personal data protection authorities - joint aspirations and cooperation, Skopje 17 -18 December 2012

The Data Protection Authority in collaboration with the European Commission Instrument - TAIEX, implemented Multi Country Workshop - "Balkan Conference of personal data protection authorities - joint aspirations and cooperation," which was held on 17-18 December 2012. The workshop was the result of the activities of the Data Protection Authority and the efforts to strengthen international co-operation in order of application of the principles of personal data protection and harmonization of national legislation novelties in EU legislation. The idea to organize a Balkan conference came from the meeting of the supervisory authorities for the protection of personal data in the framework of the Conference on the Modernization of EU legislation on the protection of personal data, which was held by the Data Protection Authority in May 2012. At this conference it was suggested organizing Balkan Conference of personal data protection authorities, through which will start with a regular annual meetings of Balkan personal

data protection supervisory authorities, as a platform for exchange of experience in legislation and practice for the protection of personal data, as well as for cooperation with the European authorities for personal data protection.

The workshop was aimed for representatives of supervisory authorities for data protection and free access to public information in the Western Balkan countries, which endorsed the Declaration of Cooperation. Particular emphasis was givven on the joint application of the Balkan authorities to use support from the IPA funds. The working part of the conference was devoted to the transfer of personal data to third countries, supervision of transmission and cooperation with Eurojust as well as the balance between the right to protection of personal data and the right of free access to public information and the need for various legal services for the realization of these two human rights. ISO standardization of the employees in bodies for protection of privacy, as a modern condition for efficient operation and execution responsibilities was also discussed.

Use of EU Funds

- ***Finished IPA 2008, Component 1, Project – Support to Directorate for Personal Data Protection***

DPDP was 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 was 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. The duration of the project was 18 months and it was finalized in June 2012.

- ***IPA 2009 program entitled "Sustainable system for continuing education in primary and secondary education, the right to protection of personal data" – on going***

The implementation of the project started by using funds through mechanisms for project preparation (PPF) from the IPA 2009 program entitled "Sustainable system for continuing education in primary and secondary education, the right to protection of personal data". The objective of the project is to assist the DPDP in the process of drafting of data protection educational materials that will be used by the students and teachers/professors in the primary and secondary education. The assignment will also support the development of an efficient mechanism for awareness raising in the educational system regarding the Personal data protection as one of the EU values and fundamental human rights.

- ***IPA 2012 program - Sector Fiche Justice and home affairs, measure 6***

The DPDP is one of the beneficiaries of the Sectoral Fiche for IPA 2012 – 2013. The aim of the project activities is to support the implementation of the Strategy for personal data protection. The implementation of these project activities is foreseen for 2014.

- ***IPA 2011 program: proposals for PPF***

A project proposal summary was submitted to use PPF from IPA 2011 "develop policies to implement the principles of protection of personal data by the media. A description on competencies is prepared in accordance with the abovementioned proposal.

A project proposal summary is submitted to use IPA 2011 program funds for the preparation of technical specifications for procurement, provided in a measure 6 of Sector Fiche 2012-2013".

- ***"Technical Assistance for strengthening the organizational and institutional capacities for protection of personal data" – on going***

A contract is signed to use the financial support of the Ministry of Foreign Affairs of the Kingdom of Norway, for the implementation of the project "Technical Assistance for strengthening the organizational and institutional capacities for protection of personal data". The project that starts in September 2013 has a duration of 18 months.

Support Instrument for technical assistance and exchange of information (TAIEX) of the European Commission

Within the requested support from TAIEX, during the reporting period several study visits and workshops were organized.

1. Study visit on the Ombudsman and free access to public information related issues, Stockholm, Sweden
2. Workshop on Privacy for politically exposed persons, 9-th of October 2012 Skopje, Macedonia
3. Workshop on Privacy in the workplace, October 19, 2012, Skopje,Macedonia
4. Study Visit to protect privacy in the educational system, 7 to 9 November 2012 Lisbon, Portugal
5. Workshop on establishing a framework for auditing the personal Data protection (Privacy Audit Framework), 12-13 November 2012, Skopje, Macedonia
6. Study Visit for European Privacy Seal, 19 to 20 November 2012 Kiel, Germany
7. Workshop on adequacy assesment, 3 -4 December 2012, Skopje, Macedonia
8. Study visit on various aspects of implementation of the legislation on protection of personal data (28 to 30 May 2013 Budapest, Hungary)
9. Study visit on protection of personal data in the Schengen Information System (21 -22 May 2013, Prague, Czech Republic)
10. Study visit of Data Protection Officer of EUROPOL and DPO of EUROJUST (21-23 July 2013, The Hague, Kingdome of Holland)
11. International Workshop on Data Protection and Internet - New Challenges (21 to 22 June 2013 Zagreb, Croatia)
12. Workshop for Civil and Criminal liability for violation of the law for protection of personal data (29 to 30 May 2013 Skopje)
13. Workshop on Video Surveillance in the institutions (May 10, 2013, Skopje)

National projects

- ***Consumer Day 2013 – Your privacy is safe with us!***

On the occasion of celebration the Consumer Day 2013, aiming to rise the public awareness for protection of personal data of the consumers in the banking sector and in the debt managing sector, the Data Protection Authority for Personal Data Protection in cooperation with the National Bank of the Republic of Macedonia, Organization of Consumers, 3 debt managing companies and 10 banks organized Open days – protection of the privacy rights of the

consumers under the motto “Your privacy is safe with us”. For more information, please visit our web site www.privacy.mk

The Open days were held on 15 March in Skopje, 19 March in Bitola, 21 March in Kavadarci, 26 March in Tetovo, 28 March in Ohrid and 30 March in Strumica, from 12:00 to 15:00 pm.

During the Open Days, the citizens had the opportunity to be informed about their right to protection of their personal data in in the banking sector and in the debt managing sector, to get answers to the frequently asked questions related to the collection and the processing of the personal data and the direct marketing and to ask direct questions to the Data Protection Authority and the Organisation of Consumers.

Trainings

In the reporting year, the Commission for the implementation of training in the Data Protection Authority, acting in accordance with the Guidelines on the organization and implementation of training for controllers and processors, 40 trainings were organized in 2012 and conducted for providing security and protection of personal data processing. 723 participants from 289 controllers and processors attended the trainings , out of which 111 from public sector and 178 controllers from private sector. Additionally, in the first half of the 2013 28 trainings were realized

Staff capacity

Strengthening the powers and competencies of the Data Protection Authority with amendments to the Law on Protection of Personal Data in 2010 and the amendment of the Rules of the work of the Government ("Official Gazette of the Republic of Macedonia" br.170/011), requires strengthening the staff capacity. In the period from June 2012 - August 2013 one civil servant has left the Data Protection Authority, and one civil servant came into office from other institution to the operating position- advisor in the Department for EU integration, projects and international cooperation.

Currently, the Data Protection Authority has totally employs of 24 civil servants. The employments in the Directorate have been made with respect to the principle of equitable representation of communities. Staffing is certainly insufficient, taking into account the current situation and the increased responsibilities of the Data Protection Authority as a unique and independent authority for the protection of personal data in the country.
Yours sincerely,

Dimitar Gjeorgjievski
Director

International Data Protection Day, 28 January 2013

In celebration of Data Protection Day, Lord McNally, Justice Minister with responsibility for data protection policy, attended the launch of the fourth edition of Rosemary Jay's book *Data Protection Law and Practice*, the authoritative guide to data protection legislation. This was also attended by the UK's current Information Commissioner and all three of his predecessors, which was a unique event.

UK Impact Assessment on the proposed EU General Data Protection Regulation

The UK carried out its own Impact Assessment of the costs and benefits of the proposed data protection instruments. While there are benefits from the Regulation, such as a reduction in legal fragmentation, the UK Impact Assessment concludes that these benefits are outweighed by the costs of additional administrative and compliance measures that the Regulation introduces. The Impact Assessment concludes that the Regulation in its current form could have a net cost to the UK economy of £100-£360 million per annum (in 2012-13 earnings terms).

January 2013 - Response to the Select Committee report published

The House of Commons Justice Committee published its opinion on the European Union Data Protection framework proposals on 1 November 2012. The Government's response to Parliament was published on 1 January 2013. With regard to the Committee's call for consistency between the two proposed instruments, the Government believes that, as far as it is possible, the principles in the two instruments should be harmonised. It is, however, important that the different contexts in which the instruments have been proposed are considered.

Stakeholder Advisory Panels

The UK has established an active Stakeholder Advisory Panel to discuss views on the new proposed EU Data Protections instruments, members of which include representatives from areas such as business, IT services, financial services, representative bodies, research and civil rights societies. Two meetings have been held, in November 2012 and July 2013. A subgroup of the Panel was convened in April 2013 specifically to discuss the issue of pseudonymous data. These views have been used to inform the UK Government's position on the proposed legislation.

Privacy Laws & Business 26th Annual International Conference 1-3 July 2013

Lord McNally, UK Minister of State for Justice and Deputy Leader of the House of Lords, attended the 26th Annual International Conference organised by Privacy Laws & Business, entitled *Bridging Privacy Cultures,* which was held at Queens' College, Cambridge. This was attended by regulators, decision makers, lawyers and privacy professionals from many countries Lord McNally spoke to the conference on the theme of *Balancing individuals' data protection rights and encouraging an enterprise culture.* Others of the 40 speakers included Seamus Carroll, Chair of the Council of Ministers' Data Protection Working Group during the Irish EU Presidency; Jennifer Stoddart, Privacy Commissioner of Canada; David Smith, Information Commissioner's Office, UK; Jacob Kohnstamm, Chairman, EU Art. 29 Data Protection Working Party; and Sophie Kwasny, Data Protection Unit, Human Rights and Rule of Law, Council of Europe.