COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 8 November/novembre 2011

T-PD (2011)07MOS

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
DG I – Droits de l'Homme et Etat de droit

INDEX / TABLE DES MATIERES

ALBANIA / ALBANIE

1. Legal Approach

The Commissioner's Office pursuant to the enforcement of the Law "On Personal Data Protection":

o **There is drafted and approved Instruction No. 8 dated 31.08.2010 "On the action of the controller, the Albanian adoption committee, before the to the processing of personal data."**

This act has as object, the instruction of the Albanian Adoption Committee in the protection of personal data. Instruction sets security measures for data storage and on protecting, in a strictly way, the confidentiality of data. Also are included the criteria of transferring of the data from the Albanian Adoption Committee to intermediary agencies and any other organ because of the duty, they have information about adoption.

o **There is drafted and approved Instruction No. 9, dated 15.09.2010 "On the fundamental rules concerning the protection of personal data in the print media, visual and audiovisual."**

This instruction is addressed to the public and private controllers that operate in the print and visual media. Instruction determines that the processing of personal data should be conducted in accordance with fundamental human rights, the right to privacy and the right to private and family life. Particular attention is set to the carefulness that print media, visual and audiovisual should have on the non publication of inaccurate, misleading or distorted information, including photos.

o **With order no. 114, dated 30.12.2010 has been prepared and approved in collaboration with INSTAT, the Code of Ethics of this institution.**

The draft of the Code of Ethics is intended to define the rules of conduct of the INSTAT employees, during the performance of duty, based on impartiality, reliability, professional independence, confidentiality and transparency, which ensure a balance of respect for human rights and fundamental freedoms of the person, in particular the right to maintain privacy, freedom and right guaranteed and research in the field of statistics and science.

o **It has given a legal opinion on the law no. 10358, dated 16.12.2010 for some amendments to Law no. 9695, dated 19.03.2007 "On adoption procedures and the Albanian Adoption Committee."**

Suggestions made by Commissioner for Personal Data Protection data are included in a separate article in title "for the protection of personal data".

o **It has given its legal opinion on the general rules of the prisons, which was approved by the Decision of Council of Ministers No. 73 dated 02.02.2011 "On some amendments to the Decision no. 303, dated 25.03.2009 of the Council of Ministers "On approval of the General Regulation of Prisons", as amended.**

Legal Opinions Commissioner for Personal Data Protection has aimed at aligning the general rules of prison by Law no. 9887, dated 10.03.2008. Changes and additions were made which

were involved in security measures to be taken and confidentiality of the Institutions of the execution of criminal judgments. It is also anticipated that the staff of the General Directorate of Penitentiary and Institutions of the execution of criminal judgments correctly implement legislation to protect personal data, including the decisions or instructions of the Commissioner for Personal Data Protection in order to achieve of an appropriate security level during the processing of personal data of prisoners through the use of labor.

o **On 17.09.2010 was signed the cooperation agreement between the Commissioner for Personal Data Protection and the Ministry of Justice. (This agreement extends its effect on institutions in the dependence of Ministry of Justice).**

The cooperation agreement aims to promote mutual cooperation to encourage and support activities of common interest. The cooperation consists in the designing of internal regulations for the protection of personal data, in drafting the regulations for the security of personal data and the preparation of codes of ethics, etc.

o **On 24.01.2011 was signed the cooperation agreement between the Commissioner for Personal Data Protection and the Ministry of Education and Science.**

The agreement of cooperation contributes to the right path to personal data protection and privacy of pupils and Albanian students. The cooperation between the two institutions will consist in establishing joint working groups formed by specialists in the field to respect the privacy principles established by law for the protection of personal data, etc.

o **It has given its legal opinion on memorandum for legal and judicial safeguards against unlawful processing of personal data which was approved in Parliament by Law no. 10 371, dated 10.02.2011 "On ratification of memorandum for legal and judicial safeguards against unlawful processing of personal data."**

The Memorandum aims to strengthening regional cooperation to expand guarantees on rights and freedoms of every individual and in particular, the right to respect for privacy, taking into accounts the increasing flow in the borders of personal data undergoing automatic processing.
Signatories to this memorandum are member states of the process of cooperation in Southeast Europe.

o **In accordance with Article 6 of Law 8503, dated 30.6.1999 "On the Right to Information on Official Documents" with the order No. 102 dated 26.11.2010 of the Commissioner, was adopted the regulation "For taking information on official documents by the public".**

The purpose of this regulation is to implement legislation on access to information on official documents and in the field of protection of personal data by the public access to official documents and ensure transparency of the administration to simplify and speed up procedures. The purpose of this regulation is to guarantee the public's right to information in a uniform, equal, fair and reasonable time, to regulate procedures for exercising the right of access by the public to official documents held by the relevant structures Office of the Commissioner.

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

o Has drafted and approved Instruction No. 10 dated 06.09.2011 “On Processing of Personal Data in Hotel Services”.

In the framework of assistance for legal acts and sub-legal acts in accordance with the law on personal data protection, experts of EU-IPA 2009 project "Strengthening of the Office of the Commissioner for Personal Data Protection" have given their assistance in the drafting Instruction " On processing of personal data in hotel services". Instruction purports to regulate the rights and obligations in context of protection of personal data of individuals collected during booking at hotels or other analog controller, motels, etc. In this instruction is determined the respective documentation that must be taken to a hotel reservation and determined that the hotel is obliged to store personal data only for a period of time that is necessary for the purpose of identity control. With the passing of this period, the hotel staffs have to destroy such data.

- **Has drafted and approved Instruction No. 11 dated 08.09.2011 "On data processing in the private sector".**

The purpose of this instruction is to establish rules on the processing of personal data of employees (collection, recording, storage, organization, adaptation, alteration, consultation, use, retrieval, blocking, erasure, destruction, transmission, etc.) employed in the private sector. This instruction will help the employers to implement the requests of the law "On personal data protection" for the prevent cases of violations of the rules of processing personal data of employees, and to guarantee the rights and freedoms of individuals, and in particular the right to privacy.

- **Has given legal opinion on draft law "For some amendments to Law no. 9157, dated 04.12.2003 "On Telecommunications interception".**

In this draft law the Commissioner has given legal opinion regarding the necessary measures to ensure the appropriate level of protection of data taken during interception as well as to maintain confidentiality in accordance with the law "On personal data protection".

- **Has given a legal opinion on " The draft agreement between the Council of Ministers of the Republic of Albania and the Government of the Slovak Republic on cooperation concerning the fight against terrorism, organized crime, unlawful trafficking of narcotic substances and their precursors and other unlawful activities ".**

The agreement aims to develop bilateral contacts, providing assistance and cooperation in the fight against terrorism, organized crime and international. Also with this arrangement is aimed the exchange of information, experience and protection of witnesses and collaborators of justice. In this agreement provides for the protection of personal data and their exchange between the States Parties.

- **Has given a legal opinion on "The technical draft agreement between the Ministry of Interior of the Republic of Albania and European Union Rule of Law in Kosovo (EULEX) on Police cooperation ".**

This agreement aims to develop cooperation in the fight against organized crime, cross border crime and other forms of it. Also with this arrangement is aimed the exchange of information, and determine their types and modes of exchange, and experience.

- **Has given a legal opinion on "Agreement for the Functioning of the National Referral Mechanism for Victims / Potential Victims of Trafficking of Persons".**

This agreement regulates the functioning of the National Referral Mechanism for the identification, referral and improve protection for victims of human trafficking and aims:

- Identification, referral, protection, assistance and reintegration of victims or potential victims of trafficking;
- Ensuring the implementation of Standard Operating Procedures for the Identification and Referral of Victims / Potential Victims of Trafficking;
- Fulfillment of all engagements, as part of a common purpose national to coordinate anti-trafficking in persons, increasing public awareness, and implementation of social and moral duty to support the reintegration of victims of trafficking.

- **Has given legal opinion on the draft law "For the voice transmissions and / or figure in the Republic of Albania".**

Commissioner for Personal Data Protection in the implementation of the European Convention for the Protection of Human Rights and Fundamental Freedoms, of EC Directive 95/46 of the European Parliament and the Council "For the protection of individuals with regard to the processing of personal data and free movement of such data " and of law no. 9887, dated 10.03.2008 "On protection of personal data," has suggested be added in the draft law respecting and guaranteeing the right to privacy confidentiality and reliability of security measures to protect personal data .

- **Has given legal opinion on the draft law “The Status of Civil Servants ".**

In this opinion we have suggested unification of terminology of this draft with the one used by the law on personal data protection. It is also proposed that the personnel files of employees who are created and managed by controllers such as the state administration institutions, independent institutions and local governments as well as file and registry which contain data, that will be administered under this law from the controller held in accordance with law on personal data protection.

- **Has given the legal opinion for the Draft Law "On electronic surveillance of persons freedom of movement restricted by judicial decision."**

The priority of this bill is to increase public safety in relation to persons who applied a different sentence from a sentence of imprisonment, then an alternative measure, or who applied a different measure of safety from arrest to prison. Commissioner's opinion is focused on the necessary measures to provide the appropriate level of protection of data subjects and to maintain confidentiality in accordance with the law "On personal data protection".

- **In October 2011 it is signed a cooperation agreement between the Commissioner of Personal Data Protection and the State Agency of Personal Data Protection of the Republic of Kosovo.**

The purpose of signing this joint declaration and a memorandum of cooperation is the promotion of mutual cooperation between our two institutions and countries in the framework of protection of personal data. Memorandum regulates the areas, manner of communication and the development of relations between the parties, in accordance with bilateral Declaration.

- **It is approved by the Commissioner the decision on the request for the authorization of the international transfer of personal data made by the representative office in Bangladesh to LM Ericsson International AB.**

In this decision are provided in detail, all facts and circumstances regarding the procedure followed and documents submitted by the applicant, the legal basis, justification and the executive part in which are provided the rights and obligations of the applicant.

- **In the quality of the member of the working group for drafting the Internal Regulation "On the Protection of Personal Data and Security in the Department of Prisons and the IEV Criminal "is prepared relevant regulations and is approved by the Director-General Order no. 496, dated 28.09.2011.**

This act aims at defining the rules and principles for the protection and lawful processing of personal data and measures for the protection of personal data managed by the General Directory of Prisons, in view of maintaining order and security and the prevention of events derived from infringement of personal data of the prisoners.

- **The authority of the Commissioner for Personal Data Protection has prepared and published the following manual:**

  - ✓ "Your Health, Your Privacy, Your Choice"

The manual is a guide for privacy and the health records. It is a guide for the public to be informed what are the health records, which health services are under the control law of the protection of personal data, what can you do if you think your privacy has been violated, etc..

  - ✓ "Personal data and your privacy at work"

The manual contains general information about employers' obligations, monitoring in the work, the right of employers to address to the Commissioner in case of dissatisfaction about how the employer deals with their personal data.

2. Awareness Raising

Office of the Commissioner for Personal Data Protection organized an activity with second-year students of journalism at the University of Tirana. During this activity, students were introduced to the Law on Personal Data Protection, the Office of the Commissioner for the Protection of Personal Data and its mission as well as legal acts passed by the Commissioner, such as Guidelines for "Processing of Personal Data in the field of Education" and Guidelines for "Printed and Audiovisual Media".

Representatives of the 9th grade's pupils and young journalists of the school's newspaper were introduced with the Supervisory Authority, the Office of the Commissioner for Personal Data Protection and concepts of privacy. Presentation of the latest news in the field of privacy on the Internet, geographic localization, giving and receiving consent, privacy and marketing etc, were introduced to these pupils. Pupils of the school "Dora d'Istria" were introduced to new risks of casual use of "social networks" in relation to creating fake profiles or/and risks that can come from inappropriate creation of a network of friends in the wider virtual environment of the Internet.

The Public Relations Directorate has coordinated with the State Television to broadcast two awareness spots on personal data protection from 22nd of February to 31st of March. This spots were conducted during 2010 with the assistance of the OSCE. Retransmission of these spots is considered an important part of awareness raising campaign for the right of personal data protection of Albanian citizens.

On 16 March 2011, the Office of the Commissioner for Personal Data Protection hosted an awareness event with students from the Faculty of Philology of Tirana University. During this activity, students of the Faculty of Philology became familiar with the Office of the Commissioner for Personal Data Protection, its mission and broad scope of protection of personal data. During the activity over 400 leaflets were distributed, among which: "Meet the Law on Personal Data Protection", "Online Banking", "How to profit in contact with the Commissioner's Office" and "Beware of the dangers in use of social networking." The event was held in the lobby of the Faculty of Philology, in a time where there was considerable presence in the number of students.

Awareness activity found wide support for students who were interested by the attracting awareness materials and talked in detail with employees of the Commissioner's Office on the scope of personal data protection and the institution of the Commissioner. Students became aware of their rights on privacy and data protection and to the possibility to address to the Commissioner's Office in case there would be a violation during the processing of their data.

On 30 June 2011, in Hotel "Monarch" in Tirana, an awareness seminar on the protection of personal data in the healthcare sector was held. A total of 31 participants were present, employees of the institution of the Ministry of Health and other institutions such as University, Hospital Center, HII, RHA, Order of Physicians, National Center of Drugs etc. In this event, representatives from the Office held presentations on: "The Law on Personal Data Protection", "Supervisory Authority: The Commissioner for Personal Data Protection", "Security is not a product but a process "," Treatment Guidelines for the Basic Rules concerning Personal Data Protection in Health Care System and the Recommendations given by Commissioner" and some practical cases were given and explained.

Also another topic titled "Protection of personal data and health data in the European Union" was held by the Czech expert Jiri Mastalka, key expert under IPA Project 2009, "On strengthening the Office of the Commissioner for Personal Data Protection". Some awareness rising materials on the field of data protection, prepared by the staff of the Office of the Commissioner, were distributed.

On 23 September 2011 on the occasion of International Day in Media Ethics, a workshop in New University (UFO) was organized. The Rector of the New University, Ambassador of the OSCE Presence in Albania, Director of the Albanian Media Institute, Chairman of the Union of Journalists and other guests from the print and visual media attended this event. On behalf of

the Commissioner's office for Personal Data Protection, the Director of Public Relations gave an opening speech where he emphasized the importance of continued cooperation of the Office of the Commissioner with the media as a valuable contribution towards the general public awareness of the importance of the field of privacy and personal data protection.

On 6 October 2011, at the premises of the Commissioner's Office for Personal Data Protection, a seminar on "Security of Personal Data Controller, as the primary task and processors in the Police Sector" was held. This seminar was attended by specialists from the Department of Defense Center of Processing and Data. The staff of the Commissioner's Office presented various topics that affect the wide field of protection of personal data. During the workshop, the participants discussed extensively with IT specialists of the Office of the Commissioner on concrete cases of violation of security of personal data and the measures necessary to minimize these risks.

On 14 October 2011, at its premises, the Office of the Commissioner for Personal Data Protection conducted a Press Release in the presence of some of the leading visual media in the country. The purpose of this report was to inform the general public about its 6 months progress (April - September 2011) the Commissioner for Personal Data.)

3. Executive Measures

In order to implement in as practical as possible manner the obligation of all public and private data controllers to notify with the Commissioner's Office, of their processing of personal data for which they are responsible, to manage efficiently the information declared and to ensure publication of this information online with a maximum access by the public, the Office of the Commissioner has intensify its activities.

In this framework, Data Protection Authority has provided sending relevant documents to recall the legal obligation for registration for both sectors, public and private. The Office is in continuous contacts with these data controllers to guarantee that all of them notify with us and it is exploring some more efficient ways how to raise awareness among different, public and private, data controllers to comply with the duty to notify. The office has organized meetings with relevant actors as to raise awareness among data controllers concerning their obligation to notify with us. As far as the private sector is concerned, we have had meetings with different chambers of commerce (Albanian, American, Greek, etc), with unions and other organizations, as to provide their assistance on making such an obligation familiar to all controllers within their domain.

As far as the public sector is concerned, we have been in continuous contacts with central institutions, local government bodies and independent institutions both in establishing cooperation and guaranteeing the fulfilment of the notification obligation.
The office has taken special measures on the general approach towards public at large, by informing and explaining to both controllers and data subjects the very process of notification. The office has made several public announcements via printed media on the legal obligation to notify. One recent announcement, following a press conference transmitted on audiovisual media, emphasized that the data controllers have to take all there measures to insure their notifications with us within a deadline, which is 31 of December 2011. This means that the office will not tolerate any data controller if deadline is not met.

Statistical Table

Notifications	
Public Data Controllers	598
Private Data Controllers	1560
Total	2158

Register	
Public Data Controllers	500
Private Data Controllers	1275
Total	1775

In relation to effective powers of intervention of the Commissioner's Office for Personal Data Protection as a supervisory authority, for the period in question we present the following information:

The Office handled overall 30 (thirty) complaints filled by personal data subjects, 10 (ten) of these complaints are filed by the data subjects (complainant) officially in a written form. There have been written answers for these complaints by the Office to the data subjects. The complaints treated by the Commissioner are of various objects.

Overall of 20 (twenty) complaints are filed by the data subject via phone and e-mails. In these cases the Commissioner has handled the complaints by giving to the data subjects the relevant instructions, for in most of these cases there was no basis for further verifications or starting administrative inspections.

For the period January- November, 2011, based on orders issued by the Commissioner for Personal Data Protection, by Department of Investigation & Inspection, are exercised administrative controls in 25(twentyfive) controllers, such as: " Conad Shqipëria" sh.a – Tiranë; " Real Estate in Albania"-Tiranë; "OMNIX Contracting & Engineering" –Durrës; " Intersig " sh.a-Tiranë; "DNA& Grey " sh.p.k – Tiranë; " Albtelecom" sh.a- Tiranë; " Wester Atlas International"-Tiranë; " Porti Detar "-Vlorë; " Konsullata e Përgjithshme Shqiptare"- Selanik, Greqi; " Drejtoria Rajonale e Shërbimeve të Transportit Rrugor- Tiranë; " Instituti i Dobësimit Orchide "- Tiranë; " Savatours" sh.p.k – Tiranë; " Euromax" sh.p.k- Tiranë; " Pelican Security"- Tiranë; "Gjimnazi Ismail Qemali"- Tiranë; "Emporiki Bank Albania S.A- Tiranë; "ALUIZNI"- Tiranë; "Gjimnazi Qemal Stafa "- Tiranë; "Spitali Amerikan" Qendra dhe Spitali Amerikan Nr. 2- Tiranë; "Qëndra Kombëtare e Transfuzionit të Gjakut"- Tiranë; "Universiteti Evropian i Tiranës"- Tiranë; "Gazeta Sot"- Tiranë; "Salloni i Bukurisë, Beauty Line"- Tiranë; "Union Bank " –Tiranë; "FIBANK"- Tiranë.

At the conclusion of these administrative controls, the Office of the Commissioner has given recommendations on where is defined the relevant deadline for their implementation. The recommendations aimed at: drafting of internal regulations on data protection and security of data; placing public notices in relation to monitoring-recording cameras (CCTV); technical security of data; fulfillment of the obligation to notify to the Commissioner's Office; obtaining consent and fair legal treatment of data subject as to clients (personal cards to customers) in terms of shopping centers; the time retention of personal data by some mobile phone operators. Some of the Commissioner's orders as well have sought to blocking and deletion of data in 2 (two) cases of mobile companies.

Department of Investigation & Inspection is making the verification in controllers for the fulfillment of the recommendations issued in this controllers, 4(four) verifications are currently made and other are in process.

Besides the abovementioned, the Department of Investigation & Inspection has proposed to the Commissioner under the imposition of sanctions, pursuant to Articles 21-23, 30 / 2, 39 / 1.4, 40 and 41 of the Law nr.9887, at 10:03. 2008 "On Protection of Personal Data" has imposed fines in 19 (nineteen) controllers, for not notifying their processing to the Commissioner's Office.

4. European and International Involvements

o Events and Cooperation.

The Commissioner's Office has actively participated to various European and International activities, such as: The International Conference of DPA-s, held in Mexico City, Mexico on 1-3 November 2011; The European Conference (Spring Conference) of DPA-s, held in Brussels, Belgium, on 5 April 2011, as well as on the 13-th Meeting of the Central and Eastern European DPA-s, held in Budapest, Hungary, on 28-29 April 2011.

As far as the regional cooperation is concerned, the Commissioner's Office has signed two Administrative Agreements with the National Agency for Personal Data Protection of the Republic of Kosovo, in Pristina on 9 November 2011 and with the Agency for Personal Data Protection of the Republic of Montenegro, in Podgorica on 19 May 2011.

o Implement the EU-IPA 2009 project "Institutional strengthening of the Office of the Commissioner for Personal Data Protection".

In the framework of cooperation with experts from EU IPA 2009 project "Strengthening of the Office of the Commissioner for Personal Data Protection" is a project developed in collaboration with IPA - 2009 and was approved by the Commissioner "Commissioner's training strategy of the protection of personal data ". The strategy aims to improve the effectiveness and performance management and financial resources.
In the framework of IPA Project "Consolidation of the Commissioner for Data Protection in Albania according to EU standards" (Europe Aid/129606/C/SER / AL) are organized training workshops of the judicial sector, statistical, etc. and has provided assistance in the preparation of various sublegal acts of the Commissioner.

ANDORRA / ANDORRE

Suite à votre courrier, nous avons le plaisir de vous détailler les développements récents intervenus dans le domaine de la protection des données au niveau national.

1.- Approbation du nouveau Règlement de l'Agence Andorrane de Protection de Données.

La législation en matière de protection de données est en outre complétée par le décret du 9 juin 2010 portant approbation du règlement de l'Agence andorrane de protection des données. Ce dernier instrument précise plusieurs aspects problématiques, comme l'application de la législation andorrane aux décisions individuelles automatisées, puisque la loi qualifiée andorrane relative à la protection des données à caractère personnel ne le reconnaissait pas expressément, les transferts de données de santé ou des Registres publics, la notion d'intérêt public important, la définition du consentement et le pouvoir de sanction de l'Agence, transposant l'acquis communautaire dans notre droit national.

2.- Décision de la Commission du 19 octobre 2010 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré en Andorre

Cette décision très importante pour notre pays, a été prise après deux années de procédures. Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, l'Andorre a été considérée comme assurant un niveau de protection adéquat des données à caractère personnel transférées à partir de l'Union européenne. Dans ce cas, des données à caractère personnel peuvent être transférées à partir des États membres, sans qu'aucune garantie supplémentaire ne soit nécessaire.

Mais, au même temps qu'elle nous approche un peu plus à l'Europe, on doit être stricts sur l'accomplissement de la Loi pour que les droits et les garanties des données personnelles des citoyens européens soient traitées conforme à ses prévisions.

BOSNIA AND HERZEGOVINA / BOSNIE-HERZÉGOVINE

Personal Data Protection Agency in Bosnia and Herzegovina was established by the Law on Personal Data Protection (Official Gazette of BiH, No. 49/06) and commenced operations in June 2006.
By the Regulation on Internal Organization, 45 working places were systematized. Currently the DPA has 22 staff members, 6 of which are civil servants employed in early 2011.

Supervision

In the Reporting Period, in accordance with its responsibilities, Personal Data Protection Agency (hereinafter: the Agency) performed inspection surveillance, proceedings ex officio, acted on complaints of citizens and gave expert opinions regarding processing and protection of personal data.
The largest part of the inspections referred to the private sector (banks, micro-credit organizations, insurance companies, etc.), as well as to administrative authorities and the health-care sector. Inspection visits by supervisors identified shortcomings related to both non-fulfillment of obligations stipulated by Law on personal data protection (hereinafter: the Law) and other laws that are required to be applied in processing of personal data. A significant disadvantage related to the processing of personal data in private sector, is data processing to a greater extent than necessary to fulfill specific purposes, as well as processing in a longer period than required to fulfill the purpose of collecting the data.
As far as ex officio proceedings are concerned, most of the activities pertained to collection of copies of ID cards and the processing of personal data without legal basis, disclosure of personal information on the official web site of Controllers, disclosure of documents containing Personal Identification Number of citizens and numbers of bank accounts, processing of data in card payment. The largest number of applications are related to irregularities in the implementation of tender procedures by seeking candidates submission of Certificate of Criminal Recordings and Medical Certificate.
The largest number of complaints referred to the legality of the processing of the ID card of citizens by public authorities, utility companies, banks, lawfull processing of Personal Data in Criminal and Operational Records, the legality of publishing extracts from Birth Registers and the right to access personal information. A large number of citizen complaints show the lack of knowledge and awareness about the personal data protection.
In the Reporting Period a large number of subject matters dealing with requirements for an opinion on the part of public authorities, as well as legal and physical persons, have been processed. A great deal of expert's statements referred to the following matters: legal basis for the processing of personal data, providing Personal Information to the third party, processing of the Identification Number of citizens, processing of Personal Data in the Enforcement and Criminal Procedure, processing of personal data in Criminal Records and seeking Certificates of Criminal Recordings, use of copies of personal documents (identity cards, passports, residence registration), processing of personal data with video surveillance and video control, disclosure of personal information on official web sites.

In accordance with the Law, the Agency has established and maintained the Central Registry, which is an electronic record of basic information about the collections that Controllers manage. Its aim is to inform the data holder which personal data Controllers can process and the purpose they are going to use them for.

In the past year, the Agency has launched an initiative to amend three laws which are very important for better personal data protection, correct functioning and establishing the independent

status of the Agency. Those are the Law on Personal Data Protection, Law on Ministries and Other Administrative Bodies of Bosnia and Herzegovina and the Law on Salaries and Remunerations in the Institutions of Bosnia and Herzegovina.

Parliamentary Assembly of Bosnia and Herzegovina adopted the Law on Amendments to the Law on Personal Data Protection ("Official Gazette of BiH", No. 76/11). The reason for passing this Law is to harmonize the Law on Personal Data Protection with the legislation of the European Union and other European and International legislation on privacy. It is also one of the obligations of Bosnia and Herzegovina by the Stabilisation and Association Agreement. An Important amendment to he Law is the definition and determination of the Agency as an independent supervisory body.

The Agency regularly participates in various conferences and training related to personal data protection. TAIEX organized an IT Expert Assistance from the Saxon Commissioner for Personal Data Protection in Dresden. Also TAIEX organized three-day training in Sarajevo on different topics on data protection for newly employed civil servants of the Agency, as well as two Study Visits for our officials in Madrid.

Raising awareness on need for personal data protection

In order to raise public awareness on subject of personal data protection, three short Video Clips were produced. Development and production was financed by the European Union, while their broadcasting was financed by the Agency. They were broadcasted on three Public Services in Bosnia and Herzegovina.

In order to inform citizens, 35.000 information leaflets on Basic Principles of Personal Data Protection, were distributed in most municipalities in BaH.

Two Publications, on subjects "Right to Privacy and "Direct Marketing", were published and posted on the Official Website of the Agency.
The Agency marked the Anniversary of the European Data Protection Day 2011, as it was practice in previous years. On that occasion, we organized a Press Conference with a specially prepared information material (Annual Report on the Protection of Personal Data and the Video Clips).

A Brochure for citizens „How to Protect Your Personal Information“ was made by the Agency to raise the public awareness regarding personal data protection.

Media Cooperation

The Agency regularly informs the Media about its competence and activities, promotes work of the Agency and informs the public regarding the processing and protection of personal data. For all media inquiries, the Agency reported in time through all available means of public information: interviews, written responses, press releases and publication of Opinions and Decisions on the Official Website of the Agency. In order to better inform the public in BaH on personal data protection, the Agency established Help Desk, whose purpose is to provide phone legal advice to natural persons and legal entities.

The Agency plans to continue started activities in order to achieve more significant progress in the field of personal data protection.

CROATIA / CROATIE

(i) The right of access to information

Pursuant to the Act on Amendments to the Act on the Right of Access to Information (*Narodne novine* Nos 172/03, 144/10, 77/11) of 2 January 2011, the Agency for the Protection of Personal Data is entrusted with carrying out the jobs of an independent body's accessing information.

The number of employees envisaged to perform the jobs of protecting the right of access to information in accordance with the systematization of workplaces should be five; currently, however, there are four employees on the job.

It was concluded by the Government of the Republic of Croatia, Class No. 330-01/11-02/01, Ref. No. 5030106-11-2 on 17 March 2011 that a mandate be given to the bodies of public authority, in such a capacity under the provision of Art.3 para.(1) point 2 of the Act on the Right of Access to Information and which are mandated to act in conformity with the Public Procurement Act (*Narodne novine* Nos 110/2007 and 125/2008), to undertake their tasks in a consistent and timely manner in pursuance of Art.20 para.(1) point 4 of the Act on the Right of Access to Information.

On 27 May 2011 the Agency submitted to the Government of the Republic of Croatia its Updated report on data supplied with regard to public procurement contracts concluded and executed in compliance with the above Conclusion adopted by the Government of the Republic of Croatia, Class No. 330-01/11-02/01, Ref.No. 5030106-11-2 on 17 March 2011. According to the Report there were 1001 public authorities that delivered to the Personal Data Protection Agency the information on web sites or by using another IT medium to publicize a Survey of the contracts.

The Personal Data Protection Agency passed Criteria for establishing compensation levels pursuant to Art.19 para.(2) of the Act on the Right of Access to Information, subsequently published in *Narodne novine* No. 38/10.

At its 23rd session, which was held on 27 May 2011, the Croatian Parliament passed an Act on Amendments to the Act on the Right of Access to Information. The Act was promulgated in *Narodne novine* No. 77/2011 of 7 July 2011, and it entered into force on 15 July 2011.

The Agency took part in drafting a text for the National Programme for the Protection and Promotion of Human Rights in the Field of the Right of Access to Information.

On the occasion of the International Day of the right of access to information - "Citizens Have the Right to Know", the Agency organised for citizens a "Day of Open Doors" - a symposium along with an appropriate presentation, held on 27 September 2011. The Agency also organised a forum entitled "The right of access to information - experiences to-date and future challenges" on 28 September 2011.

In the reporting period a project entitled "Strengthen the implementation of the new Freedom of Information Act" has been launched. Within its framework a training for information officers was held in Zagreb, on 28 October 2011. The Agency took an active part in it, both organising and holding presentations.

(ii) The protection of personal data

THE ACT ON PERSONAL DATA PROTECTION

Following the legislative procedure, **the Act on Amendments to the Act on Personal Data Protection was adopted by the Croatian Parliament at its 24th session, which was held on 28 October 2011.**

Having analysed the Act on Personal Data Protection (hereinafter referred to as Personal Data Protection Act - PDPA)(*Narodne novine* Nos 103/03, 118/06 and 41/08) and having compared it with the 95/46/EC Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24 October 1995), within the IPA 2007 project "Capacity building of the Croatian Agency for Protection of Personal Data", the Agency presented a draft of the Act on Amendments to the Act on Personal Data Protection with a view to the PDPA's becoming fully harmonized with the above 95/46/EC Directive.

The provisions of the Act in question were aimed, inter alia, at the strengthening of the Agency's supervisory powers, the harmonization of the PDPA provisions with the provisions of special laws, the reinforcement of the status of personal data protection officers with personal data controllers, a clearer definition of individual PDPA provisions, the Agency's improved work transparency, as well as the strengthening of its independence, the stated being the major objectives also recognised within the framework of the IPA 2007 "Capacity building of the Croatian Agency for Protection of Personal Data" project.

In conclusion, the legislative framework of personal data protection in the Republic of Croatia, that is, **the Act on Personal Data Protection per se has been fully harmonized with the 95/46/EC Directive after the adoption of the related Act on Amendments to the Act on Personal Data Protection.**

PROJECTS

A project entitled **"Enhancing capacities of the CAPPD in the field of right of access to information"** has been contracted within **the Matra-flex short-term programme** as part of the Dutch pre-accession bilateral assistance schemes. The purpose of the project is citizens' awareness-raising related to the Act on the right of access to information, as well as the enforcement of implementation measures in the field.

In collaboration with the Croatian State Archives, a project entitled **"Improving the Access to Information in Public Administration"** has been designed within the **FFRAC 2010**; its ultimate goal would be to create a point of access on the Agency's web site that would enable accessing all public authorities' reference files, as well as serve to establish an online service for deliveries of reports and for compilations of aggregate reports with statistics.

A project entitled "**Strengthen the Implementation of the New Freedom of Information Act**" has been launched within **the DIV/Reuniting Europe Programme**, funded on approval of the United Kingdom in cooperation with the Ministry of Justice of the Republic of Croatia. The purpose of the project is to train the personnel of the Agency and information officers employed with the ministries and the local self-government to gain a better understanding of their role under the Act on the Right of Access to Information.

For the purpose of the **LdV project entitled "Perception of the data protection and privacy issues by children and youth**" a questionnaire has been designed for conducting research, educational material has been prepared for pilot tests to be used in elementary schools, and the research methodology to be applied has been agreed upon.

The following has been done within the framework of **the IPA 2007 project "Capacity Building of the Croatian Agency for Protection of Personal Data**":
- A pilot project carried out in the sector of telecommunications and health care;

- Recommendations for harmonizing the Act on Personal Data Protection with the Directive, as well as Recommendations for Amendments to the Act in these sectors:
telecommunications (*Narodne novine* Nos 73/2008, 90/2011), data protection at one's workplace (*Narodne novine* Nos 149/09, 61/2011), the judiciary and health care;

- A unit responsible for personal data protection established with the Ministry of the Interior; the unit received a training;

- Risk-assessment developed concerning the information security system of the Agency for the Protection of Personal Data.

SUPERVISION

During the reporting period as stated above, (01 June 2010-31October 2011) 100 direct supervisions were carried out involving personal data controllers, of those were supervisions of personal data processing as well as of the enforcement of measures of personal data protection in compliance with Art.32 of the Act on Personal Data Protection (*Official gazette* Nos 103/03, 118/06 and 41/08, hereinafter referred to as: the Act). Furthermore, 233 supervisions were carried out with regard to information security, in compliance with Art.18 of the Act in period 01 June 2010 - 01 November 2011 .

During the reporting period the following sectors were supervised: state administration, local and regional self-government, the economy, commerce and trade, finances, education, health care and social welfare, telecommunications, and others.

CENTRAL REGISTER

Data Controllers

Situation	Period of time	No. of new	Total no. of data controllers
1 June 2010	from 2 June 2010	data controllers	on 1 November 2011
6,371	until 1 Nov. 2011	1,423	7,794

Records

Situation	Period of time	No. of new	Total no. of records
1 June 2010	from 2 June 2010	records	on 1 November 2011
13,744	until 1 Nov. 2011	3,674	17,418

PROFESSIONAL GATHERINGS

- Participation in a public forum: "Privacy protection today", held on the premises of Tribine Grada Zagreba, Zagreb, Kaptol 27 on 18 May 2011 in collaboration between the Agency for the

Protection of Personal Data, the Office for Human Rights of the Government of the Republic of Croatia, and the Faculty of Law of Zagreb University; a presentation was given on "One's personal identification number (in Croatian: *OIB*) from the angle of personal data protection", followed by replies to the participants' questions;

- Participation in a forum entitled "Citizens Have the Right to Know", held on the premises of the Agency for the Protection of Personal Data, Zagreb, Martićeva 14 on 28 September 2011; the occasion was the International Day of the right of access to information;

- Participation of representatives of the Agency in the conference "Accountability Phase III - The Madrid Project", organised by the Spanish Data Protection Authority Agencia *Espanola de Proteccion de Datos* and the U.S. Center for Information Policy Leadership Hunton & Williams LLP, held in Madrid on 25 and 26 May 2011;

- Participation of representatives of the Agency for the Protection of Personal Data at the 23rd Case Handling Workshop, held in Warsaw.

Personal Data Protection Day events

The Agency for the Protection of Personal Data organised a "Day of Open Doors" on its premises on 27 January 2011, which included getting together with citizens, their becoming acquainted with the activities, duties and tasks of the Agency, their obtaining answers to some concrete questions from the field of personal data protection, etc.;

The Agency organised The 5th European Personal Data Protection Day in the Europski dom in Zagreb, Strasbourg Hall, on 28 January 2011; a representative of the Agency, from the division concerned, gave a presentation on the "Personal Identification Number - OIB from the angle of personal data protection".

Safer Internet Day events on 8 February 2011

The Agency took part in this year's Safer Internet Day events in collaboration with e-Croatia.

The following promotional material targeting children was provided for the occasion:

* Protection of personal data on the Internet;

* Jeopardies lurking from the Internet;

* How to protect privacy on the Facebook.

COOPERATION WITH THE MEDIA

Whenever any requests are made by the media the Agency has provided timely replies as well as information relying on all public information dissemination means available: interviews, written replies, media statements, as well as pronouncements on the official web site of the Agency.

CYPRUS / CHYPRE

As regards the abovementioned subject I would like to inform you the following:

1. New Commissioner:

In September 2011 Mr Yiannos Danielides, who succeeded Ms Panayiota Polychronidou, was appointed as the new Commissioner for Personal Data Protection in Cyprus.

2. Training:

In June 2010 the Commissioner's Office, in order to implement the Council of Ministers' decision to designate data protection officers in every government department, organized and delivered training programs addressed to the designated officers.

3. Legislation:

3.1 A draft bill amending the Processing of Personal Data (Protection of Individuals) Law 2001 was prepared by the Commissioner's Office and is pending at the House of Representatives. This Bill among other things provides for the increase of the amount of the administrative penalties from €8.540 to €20.000, that the Commissioner may impose.

3.2 The Commissioner's Office in cooperation with the Office of the Commissioner for Electronic Communication and Postal Services prepared a Draft Bill amending the Regulation of Electronic Communications and Postal Services Law 2004 for transposing the provisions of Directive 2009/136/EC which amends E- Privacy Directive 2002/58/EC.

3.3 The Commissioner's Office in cooperation with the Cyprus Police is preparing a Draft Bill for the transposition of the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Prior Checking:

On going consultation with the Department of Personnel and Public Administration for the installation of biometric (fingerprint verification system) access control systems in all government Departments and public legal entities for the better control and management of employees.

Other:

The Commissioner's Office had active contributions in the frame of the consultation procedures initiated by the European Commission and the Council of Europe for the new legal framework for personal data protection in the EU and for the review of COE's Convention 108 respectively.

ESTONIA / ESTONIE

1. Estonian Data Protection Inspectorate celebrated the Data Protection Day with a conference on January, 28.

2. We released a profound recommendation on the protection of personal data used for employment purposes. This recommendation has proved to be necessary and useful in practice , it has also received positive feed-back from different interest groups. Summary is available in English, please follow the link.

3. Official notices, invitations and announcements of Republic of Estonia are published online in Official Journal. There are now proper and relevant rules in place for disclosing announcements containing personal data.

4. The provisions of Database Chapter in Public Health Act were amended in the interest of clarity.

5. The provisions of Punishment Register Act were amended. New regulation about time-limits for deletion of information concerning punishment was added. Also, the records in Punishment Register are made available to the public unless otherwise stipulated by law. The right to receive information about minors is restricted.

FINLAND / FINLANDE

INFORMATION ON THE RECENT DEVELOPMENTS IN THE DATA PROTECTION FIELD IN FINLAND SINCE THE 26th PLENARY MEETING OF THE T-PD

The action of the Data Protection Ombudsman

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

Data management has been the central theme of the guidance operation of the Data Protection Ombudsman. Finland has introduced a special accounting information procedure, which serves the leadership of organizations in their management and reporting activities and at the same time allows the Data Protection Ombudsman to more efficiently carry out law enforcement activities.

In Finland, in addition to the European Data Protection Day, a special national data security day is held as part of the national information security strategy. The goal is to improve citizens' awareness of security threats and improve their level of knowledge about the means that can be used to combat threats and how data subjects can protect their rights.

The office of the Data Protection Ombudsman has had extensive co-operation with different interest groups. Various data protection steering groups has been operated in, among others, the sectors of public health care, social welfare, telecommunications and education. Also the joint steering group of the Data Protection Ombudsman and the business life was born, which focused on topical data protection issues related to marketing and consumer relationship management. The first private-sector-organized networks of data protection experts has also started operating.

FRANCE

CE, 26 octobre 2011, Association pour la promotion de l'image et autres, n°s 317827,317952, 318013, 318051

Le Conseil d'Etat statuant au contentieux
Sur le rapport de la 10ème sous-section de la Section du contentieux
Séance du 30 septembre 2011 - Lecture du 26 octobre 2011
Association pour la promotion de l'image et autres, n°s 317827,317952, 318013, 318051

Vu 1°), sous le n° 317827, la requête et le mémoire complémentaire, enregistrés le 30 juin 2008 et le 22 juillet 2008 au secrétariat du contentieux du Conseil d'Etat, présentés pour l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE, dont le siège est 43-45 rue de Naples à Paris (75008), la CONFEDERATION FRANCAISE DE LA PHOTOGRAPHIE, dont le siège est 121, rue Vieille du Temple à Paris (75003), la SOCIETE PHOTOMATON, dont le siège est 4, rue Croix Faron à Saint-Denis (93210), la SOCIETE STUDIO PHOTO ELISABETH SARL, dont le siège est 10 ter, rue d'Alger à Le Mans (72000), la SOCIETE DUKA SARL, dont le siège est 8, rue des Etuves à Montpellier (34000) ; l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres demandent au Conseil d'Etat :

1° d'annuler pour excès de pouvoir le décret n° 200 8-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, ainsi que la circulaire n° INT/1/08/00105/C du 7 mai 2008 relative au choix des deux mille communes appelées à recevoir des stations d'enregistrement des données personnelles pour le nouveau passeport ;

2° de mettre à la charge de l'Etat la somme de 5 0 00 euros au titre de l'article L. 761-1 du code de justice administrative ;
Vu 2°), sous le n° 317952, la requête, enregistrée le 2 juillet 2008 au secrétariat du contentieux du Conseil d'Etat, présentée par M. C., Mme Ca., M. M., Mme Ma., M. C., M. B., M.V., Mme P., Mme Pe., M. Ma.; M. C. et autres demandent au Conseil d'Etat d'annuler pour excès de pouvoir le décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques ;

Vu 3°), sous le n° 318013, la requête, enregistrée le 4 juillet 2008 au secrétariat du contentieux du Conseil d'Etat, présentée par l'ASSOCIATION IMAGINONS UN RESEAU INTERNET SOLIDAIRE, dont le siège est 40, rue de la Justice à Paris (75020) et la LIGUE DES DROITS DE L'HOMME, dont le siège est 138, rue Marcadet à Paris (75018) ; l'ASSOCIATION IMAGINONS UN RESEAU INTERNET SOLIDAIRE et LA LIGUE DES DROITS DE L'HOMME demandent au Conseil d'Etat d'annuler pour excès de pouvoir le décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembr e 2005 relatif aux passeports électroniques ;

Vu 4°), sous le n° 318051, la requête, enregistrée le 4 juillet 2008 au secrétariat du contentieux du Conseil d'Etat, présentée par M. A. ; M. A. demande au Conseil d'Etat d'annuler pour excès de pouvoir le décret n° 2008-426 du 30 avril 2008 m odifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques ;
Vu les autres pièces des dossiers ;
Vu la Constitution, notamment son article 34 ;
Vu le traité instituant la Communauté européenne ;
Vu le traité sur l'Union européenne ;

Vu la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi que son protocole additionnel n° 4 ;
Vu la convention relative aux droits de l'enfant signée à New York le 26 janvier 1990 ;
Vu le règlement CE n° 2252/2004 du 13 décembre 2004 ;
Vu le code général des collectivités territoriales ;
Vu la loi n° 78-17 du 6 janvier 1978, modifiée ;
Vu le décret n° 2005-850 du 27 juillet 2005 ;
Vu le décret n° 2005-1726 du 30 décembre 2005 ;
Vu le code de justice administrative ;
Vu les autres pièces du dossier ;
Vu le code de justice administrative ;
Après avoir entendu en séance publique :
- le rapport de M. Gilles Pellissier, Maître des requêtes-rapporteur ;
- les observations de la SCP Thouin-Palat, Boucard, avocat de l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres ;
- les conclusions de M. Julien Boucher, rapporteur public ;

La parole ayant été à nouveau donnée à la SCP Thouin-Palat, Boucard, avocat de l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres ;

Considérant que les requêtes visées ci-dessus sont dirigées contre les mêmes décisions ; qu'il y a lieu de les joindre pour statuer par une seule décision ;

Sur les conclusions tendant à l'annulation du décret du 30 avril 2008 :
En ce qui concerne la légalité externe :
S'agissant de la compétence du pouvoir réglementaire :
Considérant, en premier lieu, qu'aux termes de l'article 34 de la Constitution : « La loi fixe les règles concernant : les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques » ; qu'aux termes de l'article 4 du décret du 30 décembre 2005 que le décret attaqué modifie : « Le passeport est délivré, sans condition d'âge, à tout Français qui en fait la demande » ; que le décret attaqué qui ajoute le recueil, dans le composant électronique des passeports, de l'image numérisée des empreintes digitales de deux doigts et fixe la durée de validité des titres ainsi que leurs modalités de renouvellement, ne pose aucune condition à la délivrance de ceux-ci ; qu'il n'a, par conséquent, ni pour objet ni pour effet de fixer des règles relatives aux garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que, par suite, les dispositions du décret attaqué relatives au passeport électronique pouvaient être adoptées par le pouvoir réglementaire sans méconnaître les dispositions précitées de l'article 34 de la Constitution ;

Considérant, en deuxième lieu, qu'aux termes de l'article 27 de la loi du 6 janvier 1978 : « I. - Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés : … 2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification des personnes physiques » ; qu'en application de ces dispositions, le pouvoir réglementaire était compétent pour créer, par le décret attaqué, pris en Conseil d'Etat, le traitement automatisé relatif à la délivrance des passeports ;

Considérant, en troisième lieu, que si en vertu des stipulations de l'article 8-2 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et de l'article 2-3 de son quatrième protocole additionnel les restrictions apportées respectivement à la protection de la vie privée et à la liberté d'aller et venir doivent être « prévues par la loi », ces

mots doivent s'entendre des conditions prévues par des textes généraux, le cas échéant de valeur réglementaire, pris en conformité avec les dispositions constitutionnelles ; que les requérants ne sont, par suite et en tout état de cause, pas fondés à soutenir que ces stipulations faisaient obstacle à ce que le pouvoir réglementaire pût compétemment déterminer les modalités d'établissement des passeports et créer le traitement automatisé contenant les données relatives aux titulaires de ces documents ;

S'agissant de la régularité de la procédure suivie :
Considérant, en premier lieu, qu'aux termes de l'article 26 de la loi du 6 janvier 1978 « I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et : 1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; (…) » ; qu'aux termes de l'article 27 de la même loi : « I. - Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés : (…) 2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. » ; qu'en prévoyant que les traitements qu'il vise sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL), l'article 27 assure des garanties supérieures à celles de l'article 26 ; que, par suite, dès lors qu'un traitement automatisé a été créé selon la procédure de l'article 27, la circonstance que l'une de ses caractéristiques soit mentionnée à l'article 26 est en tout état de cause sans incidence sur la régularité de sa création ; que, par suite, les associations requérantes ne peuvent utilement soutenir qu'en instituant le traitement « TES » suivant la procédure de l'article 27 alors que, selon elles, l'une de ses caractéristiques aurait pu le faire entrer dans le champ d'application de l'article 26, l'auteur du décret attaqué aurait commis un détournement de procédure ;

Considérant, en deuxième lieu, que si l'article 18 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 prévoit que « Les avis motivés de la commission émis en application des articles 26 et 27 de la loi du 6 janvier 1978 susvisée et les actes sur lesquels ils portent sont publiés à la même date par le responsable du traitement », ces dispositions, qui sont relatives aux modalités de publication du décret, sont sans incidence sur sa légalité ; que, par suite, les requérants ne peuvent utilement soutenir que la circonstance, pour irrégulière qu'elle soit par elle-même, que l'avis de la CNIL aurait été publié quelques jours après le décret, entache ce dernier d'irrégularité ;

Considérant, en troisième et dernier lieu, que le moyen tiré de ce que la CNIL n'avait pu émettre son avis en toute connaissance de cause faute d'avoir « obtenu les éléments qui permettent de justifier la création de la banque de données dénommée « Delphine » ni les éléments permettant d'en assurer la sécurité » est en tout état de cause dépourvu de toute précision permettant d'en apprécier le bien fondé ;

En ce qui concerne la légalité interne :
S'agissant du moyen tiré de la violation du règlement (CE) n° 2252/2004 du 13 décembre 2004 :
Considérant, d'une part, qu'à la date à laquelle le décret attaqué a été pris, aucune disposition du Traité sur l'Union européenne ou du Traité instituant la Communauté européenne ne conférait à l'Union ou à la Communauté européenne une compétence exclusive pour fixer les règles relatives aux traitements automatisés de données à caractère personnel des citoyens des Etats membres ; que, d'autre part, il ressort clairement des dispositions du règlement du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments

biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres, que le décret attaqué a notamment pour objet d'appliquer, qu'il n'a pas pour objet de fixer les conditions auxquelles les Etats membres peuvent recueillir au sein de traitements automatisés les données à caractère personnel relatives à leur ressortissants ; que, par suite, la circonstance que ce règlement ne prévoie pas la création d'un traitement automatisé des données à caractère personnel figurant sur le passeport, n'interdit pas aux Etats membres de créer de tels fichiers ; que les moyens tirés de ce que les dispositions du décret attaqué relatives à ce fichier méconnaîtraient les dispositions de ce règlement ne peuvent donc qu'être écartés ;

S'agissant des moyens tirés de la méconnaissance des stipulations de l'article 8 de la convention européenne des droits de l'homme et des libertés fondamentales, de l'article 16 de la convention relative aux droits de l'enfant signée à New York le 26 janvier 1990 et des dispositions des articles 1er et 6-3° de la loi du 6 janvier 1978 ;

Considérant qu'aux termes de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui » ; qu'aux termes de l'article 16 de la convention relative aux droits de l'enfant signée à New York le 26 janvier 1990 : « 1. Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. / 2. L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes » ; qu'aux termes de l'article 1er de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. » ; qu'aux termes de l'article 6 de la même loi : « Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : / (…) 3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs » ;

Considérant qu'il résulte de l'ensemble de ces dispositions que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités ;

Considérant que l'article 7 du décret attaqué autorise le ministre de l'intérieur à créer un système de traitement automatisé centralisé des données à caractère personnel recueillies auprès des personnes âgées d'au moins six ans, lors de l'établissement ou du renouvellement des passeports ; qu'il ressort tant des dispositions des articles 7 et 8 du décret attaqué que des écritures du ministre et du procès-verbal de l'audience d'instruction que ce traitement n'a pour finalité que de permettre l'instruction des demandes relatives à ces titres et de prévenir et détecter leur falsification et leur contrefaçon ; que l'article 8 du décret attaqué précise à cette fin que « le traitement ne comporte ni dispositif de reconnaissance faciale à partir de l'image numérisée du visage ni dispositif de recherche permettant l'identification à partir de l'image numérisée des empreintes digitales enregistrées dans ce traitement. » ; qu'en vertu de l'article 5

de ce décret, les données à caractère personnel recueillies à l'occasion de l'établissement du passeport et enregistrées dans le traitement automatisé sont, outre celles relatives à l'état civil du titulaire du passeport, l'image numérisée de son visage et celle des empreintes de huit de ses doigts ;

Considérant, en premier lieu, que, conformément à sa finalité d'authentification, l'accès à ce traitement ne peut se faire que par l'identité du porteur du passeport, à l'exclusion, en raison des modalités mêmes de fonctionnement du traitement, de toute recherche à partir des données biométriques elles-mêmes ; qu'il ressort des dispositions des articles 20 et suivants du décret du 30 décembre 2005, dans sa rédaction issue du décret attaqué, que seuls les personnels chargés de l'instruction des demandes de passeports sont destinataires des données contenues dans le traitement automatisé ; que les agents chargés des missions de recherche et de contrôle de l'identité des personnes au sein des services de la police nationale, de la gendarmerie nationale et des douanes - dont il ressort d'ailleurs des pièces du dossier, et notamment du procès-verbal de l'audience d'instruction, qu'ils ne peuvent, à ce jour, consulter directement les données à caractère personnel contenues dans le traitement - ne pourraient légalement y accéder qu'aux fins de vérifier, en cas de doute, la validité ou l'authenticité d'un passeport ; que si des agents chargés de la prévention et de la répression des actes de terrorisme ont également accès, sous certaines conditions, à ces données, l'article 9 du décret attaqué prévoit qu'ils ne pourront accéder aux images numérisées des empreintes digitales ; que, dans ces conditions, la consultation des empreintes digitales contenues dans le traitement informatisé ne peut servir qu'à confirmer que la personne présentant une demande de renouvellement d'un passeport est bien celle à laquelle le passeport a été initialement délivré ou à s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport ; qu'une telle finalité peut être atteinte de manière suffisamment efficace en comparant les empreintes figurant dans le composant électronique du passeport avec celles conservées dans le traitement, sans qu'il soit nécessaire que ce dernier en contienne davantage ; que si le ministre soutient que la conservation dans le traitement automatisé des empreintes digitales de huit doigts, alors que le composant électronique du passeport n'en contient que deux, permettrait de réduire significativement les risques d'erreurs d'identification, cette assertion générale n'a été ni justifiée par une description précise des modalités d'utilisation du traitement dans les productions du ministre, ni explicitée lors de l'audience d'instruction à laquelle il a été procédé ; que, par suite, l'utilité du recueil des empreintes de huit doigts et non des deux seuls figurant sur le passeport n'étant pas établie, la collecte et la conservation d'un plus grand nombre d'empreintes digitales que celles figurant dans le composant électronique ne sont ni adéquates, ni pertinentes et apparaissent excessives au regard des finalités du traitement informatisé ; qu'ainsi, les requérants sont fondés à soutenir que les mesures prescrites par le décret attaqué ne sont pas adaptées, nécessaires et proportionnées et à demander par suite l'annulation de l'article 5 de ce décret en tant qu'il prévoit la collecte et la conservation des empreintes digitales ne figurant pas dans le composant électronique du passeport ;

Considérant, en second lieu, d'une part, qu'il ressort des pièces du dossier, notamment des écritures non contestées du ministre sur ce point ainsi que du procès-verbal de l'audience d'instruction, que le traitement centralisé des données recueillies lors de l'établissement des passeports facilite les démarches des usagers, en ne les obligeant plus à déposer leur demande de renouvellement du titre auprès du bureau qui le leur a initialement délivré, renforce l'efficacité de la lutte contre la fraude documentaire, en faisant obstacle aux demandes déposées successivement auprès de bureaux différents et garantit une meilleure protection des données recueillies, en limitant le nombre de personnes y ayant accès ainsi que les manipulations dont elles pourraient faire l'objet ; que les finalités ainsi poursuivies sont au nombre de celles qui

justifient qu'il puisse être porté, par la création d'un traitement centralisé de données à caractère personnel, atteinte au droit des individus au respect de leur vie privée ; qu'il ressort, d'autre part, des dispositions du décret attaqué que les données biométriques ne pourront être utilisées à d'autres fins que la gestion des demandes de passeports et la vérification de leur validité ; qu'ainsi qu'il a été dit ci-dessus, le traitement ne comportera ni dispositif de reconnaissance faciale à partir de l'image numérisée du visage ni dispositif de recherche permettant l'identification à partir de l'image numérisée des empreintes digitales enregistrées ; que les personnes ayant accès à ces données, aux seules fins d'authentification du titulaire du passeport, sont limitativement déterminées ; que l'interconnexion du système de traitement n'est prévue qu'avec les systèmes d'information Schengen et INTERPOL et ne porte que sur des informations non nominatives relatives aux numéros des passeports perdus ou volés, au pays émetteur et au caractère vierge ou personnalisé du document ; que la durée de conservation des données à caractère personnel est limitée à quinze ans lorsque le passeport est délivré à un majeur et à dix ans lorsqu'il est délivré à un mineur ; que le demandeur est informé des données nominatives qui ont été recueillies et peut exercer un droit de rectification ;

Considérant qu'il résulte de ce qui précède, que la collecte des images numérisées du visage et des empreintes digitales des titulaires de passeports âgés d'au moins six ans et la centralisation de leur traitement informatisé, compte tenu des restrictions et précautions dont ce traitement est assorti, est en adéquation avec les finalités légitimes du traitement ainsi institué et ne porte pas au droit des individus au respect de leur vie privée une atteinte disproportionnée aux buts de protection de l'ordre public en vue desquels il a été créé ; qu'il en va ainsi quel que soit l'âge des personnes, dès lors que la prise de deux empreintes, nécessaires à l'établissement d'un passeport personnel, ne porte aucune atteinte aux droits spécifiques des mineurs ; qu'enfin, les requérants ne peuvent utilement soutenir que le décret attaqué méconnaîtrait un avis du Comité national d'éthique, qui ne s'imposait pas au pouvoir réglementaire ;

S'agissant des moyens tirés de l'insuffisante sécurisation des données et de l'illégale interconnexion des fichiers :
Considérant, d'une part, qu'aux termes de l'article 34 de la loi du 6 janvier 1978 : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès » ; que ces dispositions, qui sont relatives aux obligations du responsable du traitement dans le fonctionnement de ce dernier, ne peuvent être utilement invoquées à l'appui de conclusions dirigées contre l'acte portant création du traitement automatisé ;

Considérant, d'autre part, que les requérants ne peuvent davantage utilement soutenir que le traitement « TES » ne pourrait être régulièrement interconnecté avec les systèmes d'information Schengen et INTERPOL, dès lors que ces interconnexions ne résultent pas du décret attaqué mais du décret du 30 décembre 2005 ;

S'agissant des moyens tirés de la violation du principe de la liberté du commerce et de l'industrie et de l'atteinte à la libre concurrence :
Considérant qu'il résulte des dispositions de l'article 5 du décret attaqué, aux termes desquelles « A moins que le demandeur ne fournisse deux photographies d'identité de format 35 x 45 mm identiques, récentes et parfaitement ressemblantes, le représentant de face et tête nue, l'image numérisée de son visage est recueillie par la mise en œuvre de dispositifs techniques appropriés », que l'image numérisée du visage du demandeur qui ne fournit pas de

photographies d'identité est recueillie par les services de l'administration lors de la demande de passeport ;

Considérant que les personnes publiques ont toujours la possibilité d'accomplir les missions de service public qui leur incombent par leurs propres moyens ; qu'il leur appartient en conséquence de déterminer si la satisfaction des besoins résultant des missions qui leur sont confiées appellent le recours aux prestations et fournitures de tiers plutôt que la réalisation, par elles-mêmes, de celles-ci ; que ni la liberté du commerce et de l'industrie, ni le droit de la concurrence ne font obstacle à ce qu'elles décident d'exercer elles-mêmes, dès lors qu'elles le font exclusivement à cette fin, les activités qui découlent de la satisfaction de ces besoins, alors même que cette décision est susceptible d'affecter les activités privées de même nature ; que, par suite, l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres ne peuvent utilement soutenir qu'en prévoyant la prise directe par les agents chargés de l'instruction de la demande de passeport d'une image numérisée du visage du demandeur qui ne fournirait pas des photographies d'identité, sans que cette opération donne lieu à la remise au demandeur de ces clichés, exclusivement destinés à la collecte des données devant figurer dans le composant électronique du passeport, lequel demeure la propriété de l'Etat qui le délivre, et dans le traitement automatisé, le décret attaqué aurait porté atteinte à la liberté du commerce et de l'industrie et au droit de la concurrence, quand bien même ce dispositif aurait pour conséquence de priver les professionnels de la photographie d'une partie de leur activité liée à la réalisation des photographies d'identité exigées pour l'établissement des passeports ;

S'agissant du moyen tiré de la méconnaissance de l'article L. 1611-11 du code général des collectivités territoriales :
Considérant qu'aux termes de l'article L. 1611-1 du code général des collectivités territoriales : « Aucune dépense à la charge de l'Etat ou d'un établissement public à caractère national ne peut être imposée directement ou indirectement aux collectivités territoriales ou à leurs groupements qu'en vertu de la loi » ;

Considérant que le décret attaqué n'a pas pour objet ni pour effet de mettre à la charge d'une collectivité territoriale une dépense à la charge de l'Etat ; que, par suite, les requérants ne peuvent utilement soutenir que le décret méconnaîtrait les dispositions précitées du code général des collectivités territoriales ;

Considérant qu'il résulte de tout ce qui précède que l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres, MM. C. et autres, qui n'établissent pas le détournement de pouvoir qu'ils allèguent, l'ASSOCIATION IMAGINONS UN RESEAU INTERNET SOLIDAIRE, LA LIGUE DES DROITS DE L'HOMME et M. A. ne sont fondés qu'à demander l'annulation de l'article 5 du décret en tant qu'il prévoit la collecte et la conservation des empreintes digitales des doigts ne figurant pas dans le composant électronique du passeport ;

Sur les conclusions tendant à l'annulation de la circulaire du ministre de l'intérieur :
Considérant, en premier lieu, que le ministre de l'intérieur était compétent, au titre de son pouvoir d'organisation des services, pour prévoir par circulaire que les demandes de délivrance de passeports pourraient être faites dans 2 000 communes et préfectures dans lesquelles seront installées, par l'Agence nationale des titres sécurisés, des stations d'enregistrement des données biométriques nécessaires à leur réalisation ;

Considérant, en deuxième lieu, qu'aux termes de l'article 1er du décret du 27 juillet 2005 relatif aux délégations de signature des membres du Gouvernement : « A compter du jour suivant la publication au Journal officiel de la République française de l'acte les nommant dans leurs

fonctions ou à compter du jour où cet acte prend effet, si ce jour est postérieur, peuvent signer, au nom du ministre ou du secrétaire d'Etat et par délégation, l'ensemble des actes, à l'exception des décrets, relatifs aux affaires des services placés sous leur autorité : 1° Les secrétaires généraux des ministères, les directeurs d'administration centrale, les chefs des services à compétence nationale mentionnés au premier alinéa de l'article 2 du décret du 9 mai 1997 susvisé et les chefs des services que le décret d'organisation du ministère rattache directement au ministre ou au secrétaire d'Etat ; (…) » ; qu'ainsi, Mme Bernadette Malgorn, qui avait été nommée, par décret du 20 juillet 2006, publié le 22 juillet, secrétaire générale du ministère de l'intérieur et de l'aménagement du territoire à compter du 28 août 2006, avait compétence pour signer la circulaire contestée ;

Considérant, en troisième et dernier lieu, qu'ainsi qu'il a été dit ci-dessus les requérants ne peuvent utilement soutenir que la mise en place d'un système de prise de vue de l'image numérisée du visage du demandeur de passeport par l'Etat porterait atteinte à la liberté du commerce et de l'industrie et au droit de la concurrence ;

Considérant qu'il résulte de ce qui précède, et sans qu'il soit besoin de statuer sur la fin de non recevoir opposée par le ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, que les conclusions de l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres tendant à l'annulation de la circulaire du ministre de l'intérieur et de l'aménagement du territoire du 7 mai 2008 ne peuvent qu'être rejetées ;

Sur les conclusions de l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres tendant à l'application des dispositions de l'article L. 761-1 du code de justice administrative :
Considérant qu'il n'y a pas lieu, dans les circonstances de l'espèce, de faire droit aux conclusions présentées par l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE et autres au titre des dispositions de l'article L. 761-1 du code de justice administrative ;

D E C I D E :
Article 1er : L'article 5 du décret du 30 avril 2008 est annulé en tant qu'il prévoit la collecte et la conservation des empreintes digitales ne figurant pas dans le composant électronique du passeport.
Article 2 : Le surplus des conclusions des requêtes de l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE, de la CONFEDERATION FRANCAISE DE LA PHOTOGRAPHIE, de la SOCIETE PHOTOMATON, de la SARL STUDIO PHOTO ELISABETH, de la SARL DUKA, de MM. et Mmes C., Ca., M., Ma., C., B., V., P., Pe, M., de l'ASSOCIATION IMAGINONS UN RESEAU INTERNET SOLIDAIRE, de LA LIGUE DES DROITS DE L'HOMME et de M. A. est rejeté.
Article 3 : La présente décision sera notifiée à l'ASSOCIATION POUR LA PROMOTION DE L'IMAGE, premier requérant dénommé de la requête n° 317827, à M. C., à Mme Ca., à M. M., à Mme Ma., à M. C., à M. B., à M. V., à Mme P., à Mme Pe., à M. M., à l'ASSOCIATION IMAGINONS UN RESEAU INTERNET SOLIDAIRE, à LA LIGUE DES DROITS DE L'HOMME, à M. A., au Premier ministre, au ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, et au ministre des affaires étrangères et européennes.

Les autres requérants de la requête n° 317827 seront informés de la présente décision par la SCP Thouin-Palat, Boucard, avocat au Conseil d'Etat et à la Cour de cassation, qui les représente devant le Conseil d'Etat.

HUNGARY / HONGRIE

New Data Protection Act in Hungary

The Hungarian Parliament enacted Act no CXII of 2011 on Informational Self-Determination and Freedom of Information **("New Act")**, which will replace the currently effective Act no LXIII of 1992 on the Protection of Personal Data and the Publication of Data of Public Interest **("Old Act")** from 1 January 2012.

Similarly to the Old Act currently in force, the new legislation covers both the general material provisions of data protection as well as freedom of information. Since the New Act remains general law, the legislator may therefore derogate from its provisions through sectoral legislation.

The New Authority

Based on the New Act, a new authority named National Data Protection and Freedom of Information Authority **("Authority")** will be set up from 1 January 2012. The Authority will replace the currently existing Data Protection Commissioner. The Authority will have a president and a vice-president. The president is nominated by the Prime Minister and appointed by the President of the Republic for a period of nine years. The Authority is independent, it cannot be instructed within its competence and it shall take its measures exclusively on the basis of legislative acts.

Whereas the Commissioner's Office was only a sort of a "quasi authority", the investigative powers of the new Authority will be much broader and will have the right to impose fines of up to HUF 10 million (approx. EUR 35,000).

The Authority can initiate a data protection administrative proceeding if – based on the investigation conducted previously or otherwise – it can be substantiated that the Processing of personal data is unlawful and
a) affects a larger group of persons;
b) affects sensitive data or
c) may cause a serious infringement of interests or damages.

Territorial scope

In addition to governing scope provisions almost identical with those of the Old Act, the New Act declares that the Act shall apply if a third-country controller that is involved in the processing of personal data employs a processor whose registered address or place of business (branch) or habitual residence (place of abode) is situated in the territory of Hungary or if it makes use of equipment situated on the territory of Hungary, unless such equipment is used solely for the purpose of transit through the territory of the European Union. Such controllers shall have a representative installed in the territory of Hungary.

New legal bases

The processing and controlling of personal data will continue to be permitted only if prescribed by law or with the consent of the data subject. The latter must be based on appropriate information provided to the data subject regarding the data processing. The New Act also introduces two new legal bases for the processing of personal data by implementing Article 7(e)-(f) of the Data Protection Directive (95/46/EC). This means that even if it is impossible for the controller to obtain the data subject's consent or if obtaining this consent entails disproportionate costs, data controlling will become permitted also in Hungary if:

- the data processing is necessary for compliance with a legal obligation on the part of the data controller; or
- the data processing is necessary for the legitimate interests of the data controller or a third party, and these interests are proportionate with the interference with the rights for data privacy.

These new legal bases for data processing are contained in the European Data Protection Directive, but were missing from the current Act. This gap will now be healed by the newly adopted Act.

The New Act also provides that if personal data has been recorded with the data subject's prior consent and data processing is necessary for the data controller to perform his/her obligations prescribed by the act of legislation or for the assertion of a legitimate interest of the data controller or a third person – unless otherwise provided by law – and except where such interests are overridden by the interests for data protection of the data subject, data can be processed without further consent or even after withdrawal of consent the data subject.

Data controlling and data processing

The New Act preserves the distinction between data controlling and data processing (and also between data controller and data processor), whereas the latter is merely a technical task in order to accomplish the goal of the data controlling.

Sub-contracting data processing to a further data processor is still not permitted in the New Act.

Data Protection Register

As a rule, data processing must be notified to the Authority, unless notification has been exempted by the Act. If notification is a must, data processing may be commenced after the registration has taken place. The registry is kept by the Authority and the registration procedure is governed by the Act on the General Provisions of Administrative Procedure. The Authority is required to register data processing within 8 days after submitting the notification, and if the Authority does not respond within this deadline, data processing could be commenced in conformity with the filing.

Although notification cannot be considered as an authorization to processing, data processing cannot be commenced until release of confirmation on registration by the Authority or at least until the 9th day of submitting the notification sheet. This can be considered as a very important practical change, since the Old Act required only the filing of the notification sheet but not registration.

The exemptions from the mandatory notification remained basically unchanged, although financial institutions (banks, insurance companies), community service providers and electronic communication service providers having customer relationship will be required to notify to the registry their data processing activity relating to customer data. The notification is necessary for each of the different purposes of the data processing.

It must be noted that the Authority will charge a fee for data protection registrations. The service fee will be determined in a decree of the Minister of Justice.

Data protection audit

The New Act provides for the possibility of a data protection audit on the part of the Authority for a charge specified in the decree of the Minister of Justice. Unless otherwise requested by the applicant, the findings of the audit and the evaluation made by the Authority shall be published.

Conference of Internal Data Protection Officers

The New Act also introduces the Conference of Internal Data Protection Officers which is headed by the President of the Authority and secures the information exchange between DPOs.

Security of Data Processing

As for the security of data processing, the New Act contains rules that are more detailed than those of the Old Act were. For example, during the automated processing of personal data, the data controller and the data processor are required to ensure that e.g.
a) no unauthorized data entry takes place;
b) no unauthorized use of automated data processing systems occurs;
c) to which bodies personal data have or may have been transferred can be tracked and recovered;
d) who entered the data into the automated data processing system and when such entry took place can be tracked.

IRELAND / IRLANDE

Major developments in the data protection field since the 26th meeting of T-PD

In July 2010, the Data Protection Commissioner issued a Code of Practice covering Personal Data Security Breaches under section 13(2)(b) of the Data Protection Act 1988 requiring notification of significant data security breaches. The Commissioner also issued a Guidance Note in relation to reporting such breaches. The Code gives effect to one of the recommendations of the Data Protection Review Group which was set up by the Minister for Justice and Equality to examine whether legislative changes were needed to address the issue of data breaches.

The Code of Practice and Guidance Note are available on the Data Protection Commissioner's website: www.dataprotection.ie.

During 2010, the Office of the Data Protection Commissioner received 410 data security breach notifications from 123 different organisations (up from 19 notifications from 86 organisations in 2009). The Data Protection Commissioner is of the opinion that the increase reflects the more exacting demands placed on organisations by the Code of Practice rather than an increase in the absolute number of data breaches. The Office of the Data Protection Commissioner has received over 1,000 breach notifications up to 8 November 2011.

ITALY / ITALIE

The main areas of activity for the Garante in the course of 2010 - 2011 were the following:

- health care (electronic health record and health file, on line examination records, booking and collection of examination records in pharmacies, scientific and pharmacological research, project of epidemiologic surveillance on soldiers in Bosnia, collection of Hiv data in health care institutions, privacy rights in hospitals/health care institutions, storage of medical documents);
- public administration (dissemination of data on real estate owned by public entities, transparency of grants and salaries accorded by public administrations, on line publication and dissemination of personal data by public bodies, data base on pedophilia, registry for homeless persons, security measures for the Anagrafe tributaria [i.e., the information system of the Revenue Service], interconnection and security of public data bases);
- marketing (unsolicited phone calls and opt-out register ["Registro delle opposizioni"], spam, fax and unsolicited e-mails);
- electronic communications (smartphones and tablets, storage of telephone and Internet data for judicial purposes, “reverse searches”, security measures, customer profiling);
- journalism and information (judiciary records reported by the press, protection of the privacy rights of children and victims of violence, data on health and sexual activity, adoption, pictures of persons under arrest, newspaper archives on line);
- employment (detection systems based on biometric data, employee location systems, monitoring employees’ use of the internet, video surveillance in the workplace);
- police and justice (judicial data as related to mediation activities aimed at conciliation of civil and commercial disputes; digital civil trial [e-justice], security measures for judicial offices, new information system for the administrative justice, CED – IT database of the Police Public Security department, air passengers’ data, security measures for the Schengen database);
- Internet (search engines, *Google Street View, Google Buzz, Facebook* and social networks, unlawful storage of internet usage data, forums and blogs, simplified security measures for small Internet service providers, *on line* profiling);
- new technologies (geo-location, RFID-based technologies);
- schools and universities (“anagrafe nazionale degli studenti” [national students’ registry], use of video surveillance in schools, publication of grades and exam results, pupils’ rankings, personal data used for enrollment with universities);
- private bodies (“tessera del tifoso” [soccer fan card], wedding agencies, *ski pass*, condos);
- corporations (transfer of data to third countries, data relating to social security, rating agencies and oversight on conflicts of interests, simplified data protection measures, information of a commercial nature);
- banks, financial institutions and insurance companies (access to clients’ data held by banks, security measures, information systems on credit histories, access to consumer credit data by EU lenders).

The Garante also approved important **guidelines** concerning, in particular, disclosure of information on legal persons; the rules to be complied with by public administrative bodies when posting administrative records and documents that contain personal data (“public administration on the internet”); and customer satisfaction measurement in the health care sector.

The DPA started a survey on the main producers of **smartphone** software systems in order to verify adequacy of the security measures in relation to the *mobile apps* developed for such systems. The replies received so far have shown that the adopted security policies diverge in many respects. The main criticalities highlighted by this survey were described in a document

called "*Smartphones and tablets*: Current scenario and operational perspectives" that was annexed to the annual activity report of the Garante for 2010.

Via a booklet called "***Cloud computing***: guidelines for a knowledgeable use of these services", the Garante provided initial guidance for the users of *cloud computing* services (e.g.: need for prior risk-based assessment, also including reliability of the individual provider; check of the specific contractual clauses including the location of the cloud server, the typology of services offered, and training of the personnel in charge of data processing) in order to foster the mindful use of such services and with a view to providing specific rules on security measures in the near future.

Video surveillance: this issue was recently addressed by a **general decision** of 27 April 2010, which is binding on both public and private entities with a view to the installation of CCTV and video surveillance systems. The rules set forth in this general decision provide specific safeguards for the privacy of the individuals whose data are collected and processed via such systems. The decision of April 2010 replaces a previous one issued by the DPA in 2004 to take account not only of the supervening legislation, but also of the new technologies and the substantial increase in the use of video surveillance for multifarious purposes. Special attention was given to measures informing data subjects that CCTV cameras are in operation in the areas/premises they are about to access (obligation to provide specific information notices, except in case of CCTV cameras in use for public security purposes) and to the limits on retention of data collected by CCTV cameras and video surveillance systems (the images, where recorded, should be kept for a limited period of time, which should not be in excess of 24 hours. A longer retention period is envisaged in specific cases, such as police and judiciary investigations, security of banks, etc.).

LATVIA / LETTONIE (Data State Inspectorate)

Within the year 2010 the amendments to the Personal Data Protection Law have been adopted by the Parliament of the Republic of Latvia on 6 May 2011 (in force since 2 June 2010). Namely the Article 10 Chapter 4 of the Personal Data Protection Law has been amended thus determining the exceptions when the personal data processing is allowed for other purposes than initially foreseen within the criminal law cases. Another important amendment is related to the decisions of Data State Inspectorate (Article 31 Chapter 2) – the challenging or appeal against the administrative acts issued by Data State Inspectorate regarding the blockage of personal data processing, as well as regarding permanent or temporary prohibition of personal data processing, does not suspend the implementation of Data State Inspectorate's decision (unless suspended with the decision of appeal's reviewer).

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

1) Draft Law on Credit Register – the opinion was provided to the National Bank of Latvia regarding the access rights of data subject to this register as at the beginning there was a restriction of these rights foreseen that does not correspond to the Personal Data Protection Law; the opinion of Data State Inspectorate was taken into account.

2) Draft Law on Debt Retrieval – due to the opinion of Data State Inspectorate, it has been determined that the information on person cannot be inserted in a credit reference data base if the person has objected regarding the existence of debt.

3) Draft law on the amendments to the Consumer Rights Protection Law – the opinion of Data State Inspectorate was taken into account where it was indicated that these draft amendments did not take into account the application restrictions of the EC Directive 2008/48/EC regarding the amount of credit and the conditions when the it is not necessary to check the creditworthiness of a costumer.

4) Data State Inspectorate of Latvia has not been taking part in different projects at the national level in order to introduce the e-health policy. However within 2010 Data State Inspectorate carried out the inspection regarding the sensitive personal data processing within the health sector. The investigations would be continued in 2011.

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 and following more complicated questions which require in-depth analysis in order to find out the best solution regarding personal data protection.

Data State Inspectorate has organised several seminars on the issues for personal data protection, for different target audiences – for instance, directors of educational establishments, teachers, etc. Data State Inspectorate provides seminars which are open for all the persons interested (3 such seminars organised in 2010).

Key figures related to Data State Inspectorate

Organisation	Data State Inspectorate of Latvia (Datu valsts inspekcija)
Chair and/or College	Director – Signe Plūmiņa
Budget 2010	266 907 LVL (aprox. 370 457 EUR)
Staff	19 (including the administrative and maintenance staff)
General Activity	
Recommendations	Regarding the recommendation – the recommendation was

	elaborated on social networks (targeted for the users of social networks).
Notifications	352 (including the notifications on amendments to personal data processing)
Prior checks	267
Complaints from data subjects	234 complaints from data subjects regarding the possible personal data protection breach. 2 complaints from data subjects from the third countries regarding their personal data processing within SIS. 22 complaints regarding SPAM (15 investigation carried out thereof).
Advices requested by parliament or government	9 (regarding the amendments to Personal data Protection Law and the elaboration of draft law on Information Technology Security 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. When is it allowed to process personal code and by whom it is allowed?
Inspection activities	
Inspections, investigations	234 complaints: Mostly people who contacted Data State Inspectorate of Latvia have indicated on possible breach of Personal Data Protection Law in the following areas: 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. The breach of Personal Data Protection Law was concluded in 42 cases and administrative fines applied. Not all the initiated investigations have been accomplished in 2010.
Penalties	Amounts (indication on whether imposed by courts or DPAs) Amounts imposed by Data State Inspectorate – 28 warnings; 14 fines – the total amount of fines LVL 14 250 (aprox. 19 249 EUR).
DPOs	
Figures on DPOs	9 Data protection officers registered. 4 exams for Data protection officers organised.

Information on case law

In 2010 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.

Data State Inspectorate has concluded that there is a need for better cooperation on the European and international level in order to fight against the data protection breach on the internet more effectively thus ensuring the rights of the citizens on their data protection.

LITHUANIA / LITUANIE

1. Recent National Developments – legal framework

1. The Law Amending the Law on Legal Protection of Personal Data
Law amending and supplementing the Law on Legal Protection of Personal Data (Official Gazette, 1996, No. 63-1479; 2008, No. 22-804) was adopted on the 12th May 2011 and has come into force on the 1st September 2011. The new wording of the Law on Legal Protection of Personal Data (hereinafter – LLPPD) establishes that the LLPPD is not applicable for the processing of personal data of the deceased people and that the data controller must ensure that personal data are processed by the precise and clear requirements, which are set in the LLPPD and other laws. Moreover, the new wording of the LLPPD establishes that while disclosing personal data under a personal data disclosure contract between the data controller and the data recipient and if data is processed by automatic means and appropriate measures intended for the protection of personal data are applicable, priority should be given to the automatic disclosure of personal data, while in the case of a single disclosure of personal data priority should be given to the electronic means of communication. Also the new wording sets that carrying out social and public surveys personal data may be processed if the data subject has given his consent. In addition, the LLPPD foresees that financial institutions, that provide financial services may disclose to each other the data subjects', to whom these financial institutions have rendered or intend to render financial services, personal data (marital status, current job position, education) for the purpose of financial risk assessment and debt management on the condition that the data subject has given his consent.

2. On the 27th November 2010 a new version of the *Law of the Government of the Republic of Lithuania* came into force. A new wording specifies changes of legal status of the Director of the State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – SDPI). New version foresees that Director of the SDPI became a state officer. According to the new version of this law the SDPI shall operate according to the strategic plan approved by the Minister of Justice. Also this law states that the Minister of Justice offers the Government to appoint or to dismiss the Director of the SDPI, to promote or impose penalties to the Director of the SDPI, also the Minister of Justice is entitled to lay a vacation for the Director of the SDPI and send him out to the duty journeys. According to this law the Director of the SDPI shall be responsible and accountable to the Government and the Minister of Justice.

3. *Law on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters* implementing Council Framework Decision 2008/977/JHA was adopted on the 21st April 2011 and has come into force on the 1st July 2011. This law ensures the protection of the fundamental rights of the natural person, particularly the right to privacy and the right to personal data protection in police and judicial cooperation in criminal matters.

4. *Resolution of the Government "On the Amendment of the Resolution of the Government No. 1156, 25/09/2001 regarding structural reforms of the State Data Protection Inspectorate, authorities empowerment, Approval of the State Data Protection Inspectorate regulations and related amendments of the resolutions of the Republic of Lithuania"*, No. 987, was adopted on the 24th August 2011 and came into force 1st September 2011. According to this Resolution the SDPI was appointed as a supervisory authority which carries out the implementation of the Law on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (Official Gazette, 2011, No. 52-2511).

5. *Law amending and supplementing the Law on Electronic Communications* (Official Gazette, 2004, No. 69-2382; 2008, No. 87-3468, No. 131-5037, No. 137-5383) (hereinafter – LEC) was adopted on the 28th June 2011 and has come into force on the 1st August 2011. The new wording of the LEC establishes that public communications networks and (or) an electronic communication service provider must immediately notify the SDPI about personal data security breach. In the notice public communications networks and (or) public electronic communications service provider must describe the personal data breach and give details of the contact, which can provide more information, and indicate the recommended measures, which can protect personal data breach and lessen the negative impact of it. The new wording of the LEC also states that if the personal data security breach may have a negative impact on the subscriber or registered user of electronic communications services or on another person's privacy or data security, public communications networks and (or) public electronic communications service provider must also notify the subscriber or registered for electronic communications service user or another person, except in cases where a public communications networks and (or) public electronic communications service provider is able to demonstrate to the SDPI that it has implemented appropriate technical measures, which were subject to the security breach of personal data. Also the new wording sets that SDPI in accordance with the conditions set out in the laws verifies how the public communications networks and (or) public electronic communications service providers complies with their duty to implement appropriate technical and organizational measures to protect the security for the services they provide and how they carry out their obligation to notify about personal data security breaches.

6. *The Resolution of the Government amending the Resolution of the Government ,,On Approval of remuneration rules for the disclosure of personal data to the data subject'', No. 288,* was adopted on the 14nd September 2011 and came into force 23nd September 2011. This resolution provides the procedure of the remuneration for the data controller or data processor when personal data is disclosed to the data subject not the first time in a calendar year.

2. Major case law

2.1 Personal Data Processing for the Purpose of Evaluating a Person's Solvency and Managing His/Her Debt

The applicant complained that the debt collection company illegally disclosed his, as the debtor's, personal data, that has been obtained from the original creditor by cession (assignment) agreement, to the data controller who process consolidated debtor files. The SDPI has decided that applicant's personal data has been legally disclosed to a third person since in accordance with the Civil Code of the Republic of Lithuania (hereinafter – Civil Code) it was assumed that the claimant was owed to the creditor and that he did not disputed the debt reasonably.

Since the applicant disagreed with the SDPI decision, he appealed to the Vilnius district court indicating that the SDPI has not properly interpreted and applied the law governing civil liability and the burden of proof rules. The applicant also emphasized that the SDPI has no right to decide the existence (non-existence) of the debt's fact.

Vilnius district court noted that the SDPI has not indicated why the applicant's debt disputation has been recognized to be unreasonable. As a result, SDPI decision was overturned and sent to the SDPI for reconsideration. The decision of the Vilnius district court was appealed against the Supreme Administrative Court of Lithuania.

Supreme Administrative Court, after considering the appeal, noted that both provisions of the Civil Code and case law confirms that, in order to claim the transfer of the legal consequences to the debtor (to be used against the debtor), the debtor must be properly informed about the assignment agreement. In this particular case, the company that has gain right to the applicant's

debt from the original creditor, may apply the provisions of the LLPPD concerning the processing of personal data for the purpose of evaluating a person's solvency and managing his debt, only if the debtor has been informed about the assignment. Supreme Administrative Court stated that since LLPPD does not provide the definition of "reasonable dispute", there is no reason to claim that if the debt is disputed once, the person must do it regularly. Supreme Administrative Court has mentioned that since the person must contest the debt to the controller, which is the creditor, his assessment of whether the person contest his debt on compelling grounds can be biased, a person may not always have evidence that he is not indebted, in particular, as in this case, after more than 10 years must be demonstrated not only the absence of debt, but also the existence of it. Since there is no agreement between the parties about the debt, a party to the other party can not adopt a binding decision. Supreme Administrative Court concluded that reasonable challenge should not necessary be based on the documentary evidence or by the competent authorities' decisions, it can be the person's written objection with the debt. The data controller is not a court or other entity entitled to assess whether the person reasonably or unreasonably denied the debt. Since parties failed to reach agreement, creditor can not individually decide on the validity of his claim. Otherwise, it will be created the situation in which the creditor carries out the same functions as court or arbitrator, as well as the plaintiff.
For the above mentioned reasons, Supreme Administrative Court dismissed the appeal of the SDPI and upheld the decision of the Vilnius district court.

2.2 Personal data security
The SDPI received a complaint in which it was stated that the state-guaranteed legal aid services (hereinafter - Office) send to the applicant documents by the simple rather than by the registered mail packages. SDPI decided that the private information was not included in the sent documents and therefore the applicant's complain was rejected. The applicant appealed against this decision. Vilnius district court ruled that the documents, which were sent to the applicant by the Office as unregistered postal items, covered just general information about the applicant, so the applicant's appeal was again rejected. The applicant appealed to the Supreme Administrative Court.
Supreme Administrative Court ruled that the term "private information" is defined sufficiently widely by the laws and as a result while deciding if the information is considered private, the content of individual case must be analyzed.
Supreme Administrative Court estimated that private information - is the information which is more or less, but inextricably linked with the private personal life, which is in accordance with an individual's personal life: a way of life, marital status, living environment, relationships with others, the individual's attitudes, beliefs, habits, physical and mental condition, health, honor, dignity, and so on. Supreme Administrative Court stated that in the determining whether the information is private, the relationship between information and person's private life should be assessed. If the information is private in nature, it must be sent to the person in a way, which minimizes the possibility that it will be disclosed to other persons.
Supreme Administrative Court ruled that the SDPI interpreted the concept of 'private information' too narrowly and did not argue why the information that was send to the applicant by unregistered mail cannot be considered as private. In this context, the Supreme Administrative Court upheld the applicant's appeal and obligated the SDPI to re-examine the applicant's complain.

3. Public awareness

3.1 European Data Protection Day
European Data Protection Day was celebrated on the 27th of January, 2011. The Parliamentary Human Rights Committee Chairman A. Lydeka has held a press conference on "New

Technologies: Challenges for human privacy". In this press conference much attention was devoted to the protection of privacy in the processing of personal data in cyberspace. Three reports on this topic were presented: “Personal data protection in Lithuania today and data protection issues within the project "Google Street View”, “The system of the SDPI electronic services” and social networks, “Video surveillance”.
The SDPI also continued the tradition to mark the European Data Protection Day by organizing conferences, seminars on the personal data protection issues for the target group of people. On the 23th of February, 2011 the SDPI together with the European Law Students Association (ELSA), Vilnius University division “ELSA Vilnius” organized a conference on "New technologies: challenges for human privacy”. The conference was devoted to the students of the Faculty of Law. During the event, the SDPI Director Dr. A. Kunčinas, Deputy Director R. Vaitkevičienė and the law firm “LAWIN” solicitor J. Zaleskis debated on the data protection in social networks, data protection issues within the project "Google Street View’’ and search services provided by the Google company. Three reports were presented to the students of the Faculty of law: Report on the State Data Protection Inspectorate activities; “Google's services and the resulting data protection problems”; “Social networks: threats to privacy and its protection”. After the presentation of the above mentioned reports the SDPI Director A. Kunčinas has carried a quiz, which tested the students' knowledge about data protection. Students who responded correctly were cheered by the symbolic gifts from SDPI.

3.2 *Conference "Protection of personal data in Lithuania: Current Issues, Problems and Prospects"*
The SDPI together with a joint stock company “Expozona” organized a conference "Protection of personal data in Lithuania: Current Issues, Problems and Prospects" on the 19th May 2011. The purpose of this event was to introduce representatives of public and private sectors with privacy and data protection issues as much as it concerns the use of technologies and disclosure of the personal data from registers. The conference was divided into two parts: the first was the presentations and questions and the second part was a separate session for the public and private sectors. The private sector for the session was moderated by the Director of the SDPI Dr. Algirdas Kunčinas. The participants of this session discussed the direct marketing and the debtors' files. Public sector representatives discussed the video surveillance and providing personal data for the media. During these sessions, the experts not only introduced the industry to a particular topic, but also suggested possible ways of solving problems, sharing their knowledge about particular issues.
The speakers participated not only from the SDPI, but also from the Residents' Register Service, the debt collection company “Lindroff Oy”, the State Social Insurance Fund Board and the Journalistic Ethics Service. 7 presentations were given on these topics: “Privacy concerns relating the use of new technologies "; “Providing personal data from public registers information systems "; "Direct Marketing"; "Video Surveillance"; “Debtors files”, “Providing personal data for the media".
Also there were discussions and the members of the conference had possibility to ask questions, to express their opinion on the issues concerned.

3.3 On the 5th May 2011 SDPI *organized seminar for employees of the Bank of Lithuania*. During the seminar issues related to the processing of personal data and its legal regulation were discussed. The representatives of the SDPI informed the participants of the seminar about complaint handling practices and personal data protection in the recent judicial decisions.
The SDPI also had a meeting with Insurance companies’ representatives on the 16th September 2011. During this meeting issues concerning the Insurance law changes and policy holder’s, beneficiaries’ and their insurance premium payer’s data processing were discussed.

On the 10th November 2011 the *SDPI held a meeting with the representatives from the Ministry of Health, the Hospital Managers Union, the Lithuanian Union of Doctors, patients' organizations and the Human Rights Monitoring Institute*. The purpose of this meeting was to discuss the use of video surveillance in the health care facilities. During the meeting, the SDPI stated that the use of video and audio recording systems in the health care poses a particular threat to a personal privacy and that the information relating to a person's health is considered sensitive personal data. Participants at the meeting agreed that video surveillance of health care is a significant problem and supported the SDPI's view that the video surveillance in the health care facilities should be very carefully used in order to avoid the violation of the patients and doctors right to privacy.

MOLDOVA

Consolidation of the legal framework for the protection of personal data, including accession to the 2001 Additional Protocol to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.

Harmonization of the national legislation to the standards on protection of personal data according to the European and international instruments.

1. On 08 July 2011, the Moldova's Parliament adopted the Law No. 133 on personal data protection, in new version (Official Gazette No. 170-175/492 of 14.10.2011 http://datepersonale.md/en/legi/). The law shall come into effect in 6 months after its publication date (the 14 of April 2012).

In fact, the new version of the Law transposes at the national level the provisions of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*a document which develops and embodies the principles of the Convention for the protection of individuals with regard to automatic processing of personal data*).

2. To avoid disagreements between the national legislation and the Law on personal data protection, on 21.10.2011 the Moldova's Parliament adopted in the second reading (*only to be promulgated by the President of the Republic of Moldova*) the Law No. 208 on amending and supplementing certain acts, in particular:

- the Law No. 1216 – XII of 03 December 1992 on state tax (*by plaintiffs exemption from the obligation to pay the state fees related to the breach of Law on personal data protection*);
- the Law No. 982-XIV of 11 May 2000 on access to information (*by excluding ambigous provisions on categories of information excepted from the need of confidential treatment assurance*);
- the Law on advocacy (*by connecting its provisions to the rule of law on the protection of personal data*).

Ratification by the Republic of Moldova of the Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001.

The additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, adopted in Strasbourg on 08 November 2001, was signed by the Republic of Moldova on April, 29, in 2010 and ratified by the Law No. 110 of 09.06.2011 (*Official Gazette No. 103-106/274 of 24.06.2011*).

Drafting and approving of the regulatory framework to ensure implementation of the recording of personal data controllers in a public Register.

In the context of the assurance of implementation process of registration of personal data holders (controllers), National Center for Personal Data Protection (the Centre) in collaboration

with the Center for Electronic Governance, began on August 2011 activities to built **Automated Information System " State Register of personal data controllers”**.

In this respect, the draft Concept of Automated Information System was designed, that has been sent for examination to Government, on November 2.

Along with developing of the technical task of Automated Information System, an European company was selected to perform activities related to the creation, delivery and implementation of software that will ensure the informatical system operation, the main objective of which is the automatization of record activity of personal data controllers, databases, informational systems and information in that are stored and processed personal data.

Implementation of the legislation on the protection of personal data and; ensuring efficient functioning of the independent data protection supervisory authority also through the allocation of the necessary financial and human resources.

Amendment and completing of the national legal framework according to the provisions on personal data protection.

In order to develop the control mechanism of impementation of personal data protection law provisions in compliance with the provisions of the additional Protocol of the Convention No. 108, on 21.10.2011 the Parliament of the Republic of Moldova adopted in the second reading (*only to be promulgated by the President of the Republic of Moldova*) the Law No. 208 on amending and supplementing certain acts, in particular:

- the Contravention Code (*by establishing contravention liability for breaching the personal data protection law and the empowerment of the Center with powers of finding body*- as provided by the art.1 para. (1) and (2) a),b) of additional Protocol- "... *the supervisory authorities have, in particular, rights to investigate and intervene and the right to sue* ...");

- Law on the approval of the statute, structure, staff-limit and financial arrangements of the National Center for Personal Data Protection (*through the delivery of skills, powers of the national authority of personal data protection and ensuring of the full independence and autonomy of the national authority of personal data protection (including of its financial independence*). This fact will allow the transposing of the provisions of the art. 1, para. (3) of the additional Protocol -"supervisory authorities exercise their functions in complete independence”.
- Law on wage system in the public sector (*through the equivalence of wage of leadership and representatives of the Centre in relation to other public authorities with similar status*).

MONACO

les développements intervenus en Principauté de Monaco en matière de protection des données depuis 2010:

Le Gouvernement monégasque a sollicité, le 11 novembre 2009, la reconnaissance du niveau de protection adéquat au sens du paragraphe 2 de l'art 25 de la directive 95/46/CE. Le processus est en cours.

La loi n° 1383 du 2 août 2011 sur l'Economie Numér ique a introduit en droit monégasque des dispositions relatives au commerce électronique, à la preuve et à la signature électroniques, à la responsabilité des prestataires techniques et à la sécurité dans l'économie numérique.
Des dispositions spécifiques ont notamment été introduites en matière de prospection directe par courrier électronique, de nature à protéger les données personnelles des consommateurs.

L'accès aux documents administratifs, dans le respect des dispositions de la loi n°1.165 sur la protection des informations nominatives, a été réglementé par l'Ordonnance souveraine n° 3.413 du 29 août 2011 portant diverses mesures r elatives à la relation entre l'Administration et l'administré. Ce texte pose également les bases des archives publiques, dont celles comportant des données personnelles, et celles de l'Administration électronique.

Les normes suivantes de déclarations simplifiées ont été adoptées ou modifiées, par arrêtés ministériels, sur présentation de l'autorité de contrôle Gestion des fichiers de paie des personnels- Gestion des fichiers de fournisseurs- Gestion des membres des associations et des fédérations d'associations- Gestion et négociation de biens immobiliers- Gestion de fichiers clients et de prospects.

L'autorité de contrôle a en outre adopté les recommandations suivantes, lesquelles sont accessibles sur son site Internet www.ccin.mc :
- Dispositifs d'alertes professionnelles sur le lieu de travail
- Déclaration des traitements d'informations nominatives concernant la " gestion des dossiers des patients par les praticiens de santé exerçant à titre libéral"
- dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale sur support individuel détenu par la personne concernée ayant pour finalité le contrôle d'accès à des zones limitativement identifiées sur le lieu de travail, mis en oeuvre par des personnes physiques ou morales de droit privé
- Dispositifs biométriques reposant sur la reconnaissance du système veineux des doigts de la main et de la main ayant pour finalité le contrôle de l'accès aux locaux sur le lieu de travail mis en oeuvre par les personnes physiques ou morales de droit privé
- Dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalité le contrôle d'accès et/ou la gestion des horaires sur le lieu de travail, mis en œuvre par les personnes physiques ou morales de droit privé
- Dispositifs destinés à géolocaliser les véhicules professionnels utilisés par les employés d'un organisme privé
- Décisions de mise en oeuvre des responsables de traitements visés à l'article 7 de la loi n° 1.165 (secteur public)
- Dispositifs de vidéosurveillance mis en oeuvre par les personnes physiques ou morales de droit privé
- Dispositifs d'accès sur le lieu de travail mis en oeuvre par les personnes physiques ou morales de droit privé.

Le rapport annuel et les délibérations de l'autorité de contrôle sont désormais accessibles sur son site internet précité.

NORWAY / NORVÈGE (Norwegian Ministry of Justice and the Police)

1- Introduction

In the following we will present an update on the major legal developments in Norway concerning personal data protection since the 26th meeting of the T-PD.

2- Review of the personal data act

The Norwegian Ministry of Justice and the Police is currently reviewing the Norwegian personal data act, with the aim of proposing amendments in areas where it is found to be necessary. The main focus of the review is protection of minors, the relationship between data protection and the freedom of expression, provisions on television monitoring and provisions on licenses to handle personal data.

The choice of issues that are addressed in the ongoing review is partly a consequence of what it is believed that the new EU directive on personal data protection will not cover. Norway is postponing a legal review of areas that are likely to be covered by the new directive, until the directive is adopted.

3- Implementation of the data storage directive

In April 2011, the Norwegian parliament decided to implement the data storage directive as part of the EEA-agreement. Prior to this decision there was a public debate on whether Norway should make use of the right to veto, which derives from the EEA agreement, against the directive.

4- New decisions from the privacy appeals board

A short summary of some decisions from the Privacy Appeals Board from the last year:

In a decision from May 2011, the board finds that it is in accordance with the data protection act to publish the identity of, and unfavorable information about, foster parents of a child in foster care on a public website. The Appeals Board interprets the exemption in the data protection act for opinion shaping expressions broadly, and finds that expressions which are protected under the constitutional right of freedom of expression are not governed by the data protection act.

In a decision from September 2011, the Appeals Board finds that the use of GPS data to control potential breaches of the overtime scheme in a company is not in accordance with the personal data act. A GPS tracking system in company cars was introduced to improve the effectiveness of the company, and neither the employees nor their organisations were informed the the GPS system together with timesheets would be used to control whether the employees were claiming irregular overtime compensation. The Appeals Board found that use of the GPS tracking data in this manner was not in accordance with the original reason that was given to the employees for introducing the GPS system. They also stated that there was no other legal basis in the personal data act that could justify the use of the information, taken into consideration that control of the employees' overtime claims could be done in a less intrusive manner.

The Appeals Board did however take note of the fact that the courts accepted the data as evidence in a case concerning the termination of the employment of the person in question, even if the court also found that the collection of data was not in accordance with the data protection act.

In a case from February 2011, the Appeals Board found that a 15 year old cannot lawfully give a consent to answer a survey that is not anonymous, where the answers contain sensitive personal information. This applies even if it increases the chances that the data material from the survey will not be representative. The Appeals Board holds that children under 18 years of age cannot give consent for others to handle sensitive personal information about themselves, the legal guardian must give an explicit and informed consent for the use of data to be lawful.

POLAND / POLOGNE

1. Summary of activity and news

In 2010 a new Inspector General for Personal Data Protection (GIODO) was appointed. On June 25th, 2010 the Sejm of the Republic of Poland appointed Dr. Wojciech Rafał Wiewiórowski to this function. After approval by the Senate of the Republic of Poland, and after taking the oath on August 4th, 2010, Dr. Wojciech Rafał Wiewiórowski assumed the duties of GIODO, thus beginning his four-year term in office. Dr. Wojciech Rafał Wiewiórowski graduated from the Faculty of Law and Administration of the University of Gdańsk, and in 2000 he was awarded the academic degree of Doctor in constitutional law.

This was also the year of legislative work on the revision of the Polish Act on Personal Data Protection, which resulted in the enactment by the Sejm of the Act of October 29th, 2010 amending the Act on Personal Data Protection.

The most significant changes introduced by the amending Act include new competencies of GIODO concerning the possibility to impose fines as an enforcement measure in order to compel those entities that do not comply with the decisions of GIODO. Also, an explicit right was added for GIODO to request competent authorities to undertake legislative initiatives and to issue or to amend legal acts in cases relative to personal data protection. Entities which received a formal position or request from GIODO are now obliged to respond to them within 30 days of their receipt. The amended provisions of the Act on Personal Data Protection introduced a new type of crime, i.e. concerning preventing or hindering the performance of inspection activities of GIODO. The punishment for this crime is in the form of a fine, restriction of liberty or imprisonment of up to 2 years, and may be imposed not only on the data controller, but also on any person who, while participating in the inspection, prevents or hinders its conduct. The effective date of the Act passed in 2010, amending the Law on Personal Data Protection, is March 7th, 2011.

2. Legislation

The Inspector General, within its scope of power, receives draft acts for an opinion. The concerns of the data protection authority are raised by tendencies of different entities to form so-called mega-databases of personal data, containing information about millions of individuals. GIODO issued opinions on legal acts, by virtue of which it is planned to introduce an information system in health care now called the Medical Information System (SIM), and the Education Information System (SIO), which from a statistical collection of data is to become a filing system containing personal data, including sensitive data of preschoolers, schoolchildren, students, teachers or the Central Register of Entities – National Register of Taxpayers involving partial “duplication” and the wider availability of Social Security database, in order to use it as a reference number also in dealing with tax authorities.

As there is a lack of single law regulating video surveillance field, GIODO is taking actions aimed at regulating this sphere with the intent to initiate legislative steps. In September 2011 GIODO prepared and send to the Ministry of the Interior and Administration an exhaustive paper entitled Requirements for rules on video surveillance.

4. Inspection activity

The Inspector General conducts inspection activities. It is worth to mention some of them:

- In the second half of 2011, a number of inspections were carried out in sport clubs and institutions involved in the organization and operation of sporting events. The purpose of these inspections was to, amongst others, set in order personal data protection issues in clubs and sports organizations before the EURO 2012.
- On May, 2011 inspection activities were carried out regarding processing of personal data by Google, Inc., headquartered in Mountain View, United States of America processed in the context of Google SreetView. The aim of the inspection was to ensure that the activities performed by Google, Inc. will comply with data protection rules. The inspection covered the processing of personal data by Google, Inc. with the use of equipment and systems meant for recording street view images.
- In June 2011, the Bureau of the Inspector General was informed about leaks of personal data from two websites providing services in the field of employment placement. As a result of inspection activities it was determined that the cause of data leakage was the lack of adequate security of processed data against interference from website copying crawlers and web browsers. In response to the incidents that took place the Inspector General issued a statement calling on Internet service providers to pay more attention to appropriate security of web services and also published a brief guidance for data controllers on how to reduce interference of crawlers in the content of the information that can be accessed on the website so that access is restricted to authorized users only.

5. Registration

In 2010 more personal data filings system were registered as compared to previous years (in 2008 – 3760, in 2009 – 6465, **in 2010 – 9921**). It was possible due to the fact that the declaration did not contain such a quantity of errors, as was the case in previous years. Undoubtedly, this result was influenced by the actions taken by GIODO that led to the modification of a computer program that assists filling the application form introduced on the basis of the Regulation of the Minister of Internal Affairs and Administration of December 11th, 2008 as regards specimen of notification of a data filing system to registration by the Inspector General for Personal Data Protection.

6. Educational activities

In 2010 GIODO continued educational activities, including:

- signing a memorandum of understanding (MoU) with the Internet Industry Employers' Association IAB Poland, which is aimed at ensuring that Internet service providers in their activities adhere to privacy principles, in particular in the form of the joint development of a code of good practice. The mainstream media websites, as well as other companies in this industry, through this MoU, want to emphasize that they care about the proper protection of personal data, so that people using different content and services on the Internet can feel safe;
- together with the Office of Electronic Communications (UKE) GIODO developed a "Guide for users of publicly available telecommunications services", which aims at meeting the needs of people who intend to take a decision to make use of certain telecommunication services, as well as those who already use various forms of electronic communication;

- organized several conferences, including the conference entitled “Reform of privacy”, which officially initiated the public debate about how to protect privacy in the era of modern technology. This public debate is meant to develop a position on the changes to be made in Polish and EU legislation on data protection and privacy rights.

In 2011 GIODO continued educational activities, including:

- the scientific conference on “Protection of personal data in schools” (Warsaw, February 6th, 2011),
- the international seminar “Binding Corporate Rules” (Warsaw, June 14th, 2011), and
- the International Data Protection Conference (Warsaw, September 21st, 2011)

The International Conference was organized by the Ministry of Internal Affairs and Administration and the Inspector General for Personal Data Protection. The conference was planned under the project, whose aim is to identify and discuss current needs regarding the data protection legal framework at European level, referring to the concrete and practical achievements in the various Member States. Conference partners were the Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information, the Hungarian Ministry of Public Administration and Justice, Council of Europe, European Commission, the Academy of European Law and the Spanish Ministry of Justice. Also, within the above mentioned project the International Data Protection Conference in Budapest was held (June 16th-17th, 2011),

- the Case Handling Workshop (Warsaw, October 4th-5th, 2011),
- Publication of the Election Guide entitled “Personal Data Protection in the course of the election campaign”,
- Within the framework of the partnership project: “Raising awareness of the data protection issues among the entrepreneurs operating in the EU” put into practice jointly by the Bureau of the Inspector General for Personal Data Protection, Czech Office for Personal Data Protection and Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information, a guide entitled “Selected data protection issues. Handbook for entrepreneurs” has been issued. Publication is directed to people conducting business activity in Poland, Czech Republic and Hungary.

SERBIA / SERBIE

Report on the latest developments in the field of data protection in Serbia
May 2010 – December 2011

1. Legal Framework

Since May 2010 there have not been changes to the Law on Personal Data Protection. The accompanying regulation, namely a bylaw on measure of storing and security of sensitive personal data is still lacking. The deadline for the Government was May 2009.

In late August 2010, the Government adopted the Data Protection Strategy envisaging the adoption of the Action Plan till November 2010, which is still lacking. The Strategy provides for bases for amending the Law as well as other regulation with European standards in the field of data protection including inter alia regulating video surveillance for non-police force use and biometric data.

In September 2010, the findings of the study on the compliance of the Law with 95/46/EC Data Protection Directive were presented, concluding that the Law needed to be amended in order to comply it with the Directive. This was confirmed in the European Commission's Progress Report for Serbia in 2010.

The Law on Electronic Communications was adopted in 2010. In September 2010 the Commissioner for Information of Public Importance and Personal Data Protection and the Ombudsman challenged the constitutionality of legal provisions enabling access to retained data without a court order. The case is still pending.

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

2. Major Cases

There were several cases that raised public concern including a draft bylaw prepared on the bases of the disputed Law on Electronic Communications, adoption of which with jeopardise right to confidentially of correspondence. There were also personal data protection breaches regarding video surveillance and employment and collection of sensitive personal data for the elections of national minorities' councils in Serbia.

Throughout 2011 the Commissioner conducted the first **Systemic Supervision** of personal data protection in Serbia. The supervised institution was the Ministry of Interior and police forces in Serbia. The report is to be finalised by the end of 2011.

3. Commissioner's Office

Commissioner for Information of Public Importance and Personal Data Protection is competent for both personal data protection and freedom of information. The specific competences differ. The number of currently employed staff is 40, while the overall number is 69.

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

4. Data Protection Day, 28 January 2011

The Commissioner hosted a one-day event hosted organised with high representatives of the Government and the Ministry of interior, Ombudsman, Council of Europe Office in Belgrade and EU Delegation to Serbia, and the Fund for an Open Society – Serbia.

5. Projects

Education of CSOs representatives – In November and December 2011 the Commissioner will organised 5-day seminar for the representatives of 20 civil society organisations. The aim of the seminar is to acquaint CSOs' representatives on personal data protection challenges and to improve knowledge and develop skills to identify personal data protection issues and provide counsel to individuals. The aim is to build up expertise within CSO in order to make them more competent in personal data issues, and project, as well to ease the task of the Commissioner in performing its duties. This mainly with regard to education and awareness rising.

Capacity building of the Office of the Commissioner – in late November 2011 a Twinning Light Project is expected to commence, 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, preparing manuals for Commissioner's and main data controllers' staff respectively as well as organising training for the staff. Small portion of the overall budget (in total €250.000) is allocated for public campaigns.

SLOVENIA / SLOVÉNIE

A. Position and competences of the Information Commissioner

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

Among other competencies determined by the ICA the Information Commissioner is the inspection and offence authority in the area of data protection in accordance with the Personal Data Protection Act[2] (PDPA), performing also specific supervision functions under special legislation in the areas of patient rights, electronic communications, public media, personal identification and travel documents etc.

B. A summary of the activity

In 2010 the Commissioner initiated 599 cases regarding a **suspected breach** of the PDPA provisions, 202 (34%) in the public sector and 397 (66%) in the private sector. Compared with previous years (624 cases in 2009, 635 in 2008, 406 in 2007 and 231 in 2006) a dramatic increase in caseload has been ceased and stabilized during last 3 years. In the public sector the most common suspected breaches involved unauthorised transfer of data to third persons, unlawful publication of data, unlawful collection of data, denied access to data subject's data and inappropriate security of data. In the private sector most suspected breaches involved abuse of data for the purpose of direct marketing, unlawful collection of data, unlawful publication of data, unlawful video surveillance and transfer of data to unauthorised third persons. Upon the examination of complaints received and due to ex officio procedures, 150 inspection procedures were initiated against public sector legal entities and 306 against legal entities in the private sector. In 2010, 179 offence procedures were initiated, of which 45 against public sector legal entities, 82 against private sector legal entities, and 52 against individuals. The number of inspection and offence procedures was similar to the previous year.

In addition to the inspection and offence authority competencies the Commissioner performs other tasks as provided by the PDPA. The Commissioner issues **non-binding opinions and clarifications** on specific issues regarding data protection raised by the individuals, data controllers, public bodies and international bodies. In 2010 the Commissioner issued 1859 opinions and clarifications, which shows a significant increase from the previous year (1334) and may be attributed to the transparent work and intensive public campaigning of the

[1] Official Gazette of the RS, No. 113/2005.
[2] Official Gazette of the RS, No. 94/2007

Commissioner. The Commissioner is under PDPA also competent to conduct **prior checks** regarding biometric measures (8 decisions in 2010), transfer of data to third countries (10 decisions in 2010) and connection of public filing systems (7 decisions). The data controllers in such cases need to firstly obtain the Commissioner's permission. The number of prior check decisions as well as applications decreased from the previous year. In 2010 the Commissioner received 85 appeals (in comparison to 48 in 2008 and 70 in 2009) concerning the **right to access** one's personal data, which shows an increase in the number of appeals. However, a decrease was noted in the number of cases due to the non-responsiveness of personal data controllers (38% of appeals in 2010 compared with 51% of appeals in 2009).

In the course of its **awareness raising activities** the Commissioner continued its preventive work (lectures, conferences, workshops for various target groups). Together with the Centre for Safer Internet of Slovenia the Commissioner covered awareness raising activities for children and young people with lectures at schools and publications. The Commissioner published **guidelines** on various data protection topics: on online forums, privacy impact assessments, guidelines for healthcare service providers and for information solutions developers. In addition, 2 brochures were published on patient's data and on data protection for consumers. In the context of the **European Data Protection Day** the Commissioner organized a round table debate that focused on direct and targeted marketing done by retailers that often invade the rights of consumers. On this occasion the Commissioner awarded 3 data controllers for good practice in personal data protection – one of the awards being dedicated to the efforts for respect of Privacy by Design principle.

In addition to the Eurobarometer survey in 2008 which proved a high level of **public awareness** on privacy issues in Slovenian citizens as well as data processors, the results of Slovenian public opinion poll Politbarometer have been constantly showing high reputation and **public trust** enjoyed by the Commissioner in the course of last years. According to the survey in 2010 the Commissioner was ranked in second place in terms of public trust in different institutions (immediately next to Euro) leaving behind all other institutions, such as Military, the President of the Republic, the Ombudsman, Schools, Police etc.

The Commissioner participated in a number of **inter-departmental work groups** in Slovenia on e-government projects, such as e-Health, e-Social services, e-VEM (portal for entrepreneurs), e-archiving and in the inter-departmental work group for the strategy of development of information society 2011-2015. The Commissioner was consulted by the legislator and competent authorities regarding 51 Acts and other legal texts.

C. Significant case law

The Ljubljana public transportation company (LPP) introduced an **e-ticketing system, based on the use of an anonymous or a personalized electronic travel card**. The company also processes passengers' location data (data on the time and place of entering the bus and data on the bus line the passenger took). The Commissioner established that in the case of a personalized travel card it is not necessary for the company to process location data as the passenger is charged a fixed monthly fee. The company did not obtain consent from the passengers and the Commissioner thus concluded that the company processed the above location data without an appropriate legal basis. The company was ordered to delete the collected location data and to adapt the system in order to no longer process such data in the future.

The Commissioner received a complaint from an individual who joined an SMS club and soon unregistered but still received commercial content. The company operating the SMS club argued that a mere **mobile telephone number cannot be treated as personal data** as it points to a device and not necessarily to a person. The Commissioner established that a mobile phone number must be regarded as personal data, as the individual is identifiable, taking into account all the means the data controller can reasonably use in order to identify the individual. Direct marketing via SMSs is only permissible with the individual's consent and the data controller must delete or render anonymous the data on individuals who have cancelled their registration. The Administrative Court later upheld this decision.

A newspaper distribution company introduced **GPS monitoring of individuals who distribute newspapers**. The company obtained the employees' consent, however if the employees did not carry the device the company would terminate their employment. The Commissioner established that GPS monitoring in this case constitutes data processing, and that the company did not demonstrate an appropriate legal basis for such. Processing personal data on the basis of personal consent is not sufficient in employment relationships, where the employer is the stronger party and the employee cannot give valid consent if threatened with the termination of the employment contract. The Commissioner ordered the company to stop using the GPS devices for this purpose.

A municipality started **reviewing video surveillance footage to detect violations in stationary traffic (illegal parking)**. The city traffic wardens did not determine violations "on the spot" but rather reviewed video surveillance footage and checked for possibly illegally parked or stopped vehicles. The traffic wardens would then establish the identity of the driver and send him/her a ticket. The Commissioner found that such conduct is disproportionate and foremost without legal grounds. The Information Commissioner prohibited the municipality from reviewing footage of the video surveillance system for the purpose of offence proceedings.

The Commissioner received a considerable number of complaints regarding **the publication of personal data in the media, on the internet, and especially on social networking sites**. The Commissioner is only competent to act in cases that concern data that is part of a filing system. That is why in most cases (e.g the existence of defamatory content on online forums, false profiles on social networks) the Commissioner only advises the individuals to complain to the police or state prosecutors competent to take action. The act of abusing personal data is a criminal offence as determined by the Penal Code of Slovenia. The injured party may also initiate a civil action before a court. In cases where such publication involved data from filing systems (such as the publication of criminal charges, medical records, etc.) the Commissioner initiated an inspection procedure.

D. Other important achievements

The Commissioner participated in a number of **international bodies**: The Article 29 Working Party, Joint Supervisory Body of Europol, Joint Supervisory Authority for Schengen, Joint Supervisory Authority for customs, EURODAC, WPPJ, International Working Group on Data Protection in Telecommunications, Council of Europe's Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). The Information Commissioner continued her work as the Vice-President of the Joint Supervisory Body of Europol.

The Commissioner was also active in the field of **bilateral international cooperation**. In 2010 it hosted a study visit of the Polish, Hungarian and Kosovo Republic representatives, and an award holder of European Fund for Balkans.

In a consortium with the Ludwig Boltzmann Institute for Human Rights from Austria the Commissioner participated in a twinning project – Implementation of Personal Data Protection Strategy in Montenegro. The project focused on establishment of a national supervisory body for data protection and establishment and implementation of the legal framework for data protection in Montenegro.

In terms of **policy issues** the Commissioner has dealt with extensively, it is necessary to mention the increasing use of video surveillance, where the Commissioner has proposed changes to the existing legislation which would better protect the individuals' rights in this regard. The Commissioner also notes that smart face recognition video surveillance is developing fast. Regarding the IT solutions in private companies and the public sector the Commissioner notes that security of such systems is often not comprehensive enough to satisfy the conditions set by the PDPA. An important issue, raising many concerns, is also the employees' right to privacy and data protection in the workplace, where the Commissioner proposed a draft of an Act on Communication Privacy in the Workplace. Special attention was paid by the Commissioner to endorse and educate the data controllers on the concept of Privacy by Design, namely in the projects of switchover to electronic commerce, the Security Information and Event Management tools, and the introduction of average speed cameras on the roads. The Commissioner also pays special attention to the development of Cloud Computing, which raises significant concerns in terms of data security and responsibilities of the data controller, and the so called Internet of Things.

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

Having in mind the importance of the proper functioning of the Data Protection Authorities, the Directorate for Personal Data Protection of the Republic of Macedonia adopted the Strategy for personal data protection 2012-2016 with Action plan for its realization and the Research on media awareness for improved implementation of personal data protection right. Both documents are the main outputs from the IPA 2008 Project "Support to drafting of strategic documents and corresponding action plans, including media awareness research, for improved implementation of the personal data protection right".

The Directorate for Personal Data Protection as the competent institution for personal data protection in our country decided to apply new mechanisms of work, to implement new methods and principles in the implementation of the legislation through the legal and institutional but moreover preventive measures and partner relations with the controllers from the public and private sector for consequent implementation of the European principles from the area of personal data protection in our country. Creation of effective, efficient and in the same time sustainable system as our vision were our challenges during preparation of the Strategy.

Regarding the Strategy for personal data protection 2012-2016 with Action plan for its realization, the Directorate for Personal Data Protection, supported by the Delegation of the European Commission in Skopje, decided to organize the International Conference on Strategic approach in development of the mechanisms for protection of personal data, which will be held on 24th and 25th of November 2011, in Skopje, Republic of Macedonia , where the issues of institutional protection of personal data can be addressed in the view of developing the needed mechanisms for data protection.