Strasbourg, 28 May / mai 2014

T-PD(2014)04Mos

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

Directorate General Human Rights and Rule of Law /
Direction Générale Droits de l'homme et Etat de droit

TABLE OF CONTENTS / TABLE DES MATIERES

ALBANIA / ALBANIE

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD IN THE AUTHORITY OF THE COMMISSIONER FOR PERSONAL DATA PROTECTION FOR THE PERIOD JULY 2013 - APRIL 2014

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

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

- Has drafted and approved Instruction No.36, dated 05.07.2013 on "Some rules for processing personal data in Official Statistics";

The instruction regulates certain rights and obligations of controllers that operate statistics under the Law No. 9180, dated 5.2.2004 "On official Statistics". The need for the adoption of this instruction has arisen as a result of the developments and frequent impact of personal data processing in the areas of activity of the statistics in the Republic of Albania.

- Has drafted and approved Instruction No. 37, dated 10.07.2013 "On protection of personal data during processing of fingerprints by public institutions";

The purpose of this instruction is to establish binding rules to the public institutions for the collection and processing of fingerprints of the employees, for the verification of the employees attendance (entry or exit from the institution).

- Has drafted and approved Instruction No. 38, dated 05.08.2013 "On the actions of the Albanian Adoption Committee, prior to the processing of personal data";

In the framework of the amendments to the Law No. 9887, dated 10.03.2008 "On protection of personal data" it was found reasonable the abrogation of Instruction No. 8, dated 31/08/2010 "On the actions of the controller, Albanian Adoption Committee, prior to the processing of personal data" and the approval of a new act.

- Has drafted and approved Instruction No. 39, dated 05.08.2013 "On processing of personal data in public registers";

The purpose of this instruction is to establish the mandatory rules to be implemented by public institutions regarding the collection, processing and publication of personal data containing public records.

- Has drafted and approved Decision No.6, dated 05.08.2013 "On determination of detailed rules for personal data security".

Following the amendments to the Law No. 9887, dated 10.03.2012 "On protection of personal data", approved with the Law No. 48/2012, the approval of two specific instructions which define in details the security measures that small and large controllers should undertake, it was found reasonable the abrogation of Decision No. 1, dated 04.03.2010 "On determination of detailed rules for personal data security" and the approval or Decision No. 6.

- Joint Instruction approved by KMDP and the Ministry of Internal Affairs “On appointing the institutions and bodies which receive personal information from the Civil Status service, and on the way, kind and amount of information they should receive”.

This instruction determines the institutions which have access to the registry of Civil State, the legal base on these cases, purposes for which they use personal data, their amount and kind.

- Has drafted and approved Strategy 2014-2017.

For the following years 2014-2017 the Institutional Strategy was approved, aiming to crystallize the vision of the Authority of the Commissioner for the next 4 years, based on a transparent highlighted progress, through priorities translated into concrete objectives. The action plan attached to this Strategy outlines the key commitments provided following their deadlines.

- Pursuant to the Law No. 9887, dated 10.03.2008 “On personal data protection”, as amended, the Authority of the Commissioner has presented to the Commission of Legal Issues and Public Administration of the Assembly of Albania the annual Report related to the activity of the Commissioner for Personal Data Protection for 2013.

- Has drafted and published summary with all the practical cases prepared serving for implementing the instructions approved by the Commissioner for Personal Data Protection, which will be sent to all the Data Protection Officers;

- Has drafted and approved Guidelines on processing of personal data in public administration;

- Has drafted and approved Guidelines on knowledge concerning biometric data (appendix: biometric data in the workplace);

- Has drafted and approved Practical Guide for Data Protection Officers;

- Has drafted and approved changes of the manual “On evaluation of the applications for approval of data transfer in foreign countries”;

- Has drafted and approved communication channel between the Commissioner for Personal Data Protection and the Data Protection Officers;

- Has drafted and published questionnaire for small and large processing entities, in the framework of implementation of Instructions No. 21 and No. 22 approved by the Commissioner;

- Has drafted and published questionnaire for processing entities, in the framework of international transfer of personal data;

- Has drafted and published the document “Privacy protection policy”;

- Has drafted and published second volume of the Legal Summary of the Commissioner for Personal Data Protection;

- Has drafted and published additions and amendments of the “Model Confidentiality Declaration” which is also published on the official website of KMDP.

- On January 2014 was signed the Cooperation Agreement between the University of New York Tirana and the Authority of the Commissioner for Personal Data Protection;

Through this agreement is intended the mutual information on latest news and institutional developments, experiences exchanges, incitement and assistance on personal data protection legislation and the organization of joint activities of mutual interest.

- On February 2014 was signed the Cooperation Agreement between the Authority of the Commissioner for Personal Data Protection and the National Agency for Information Security;

Through this agreement is intended the creation of an interagency collaboration including other public and private sector stakeholders, aiming to promote the culture of safe internet, the exchange of relevant information to the extent permitted by the respective legislation, engaging in joint inspections, etc.

- On March 2014 was signed the Cooperation Agreement between the Authority of the Commissioner for Personal Data Protection and the National Employment Service.

The object of this agreement is strengthening of the cooperation and coordination of the activities of both institutions in the framework of general human rights and freedoms protection, in the field of personal data protection.

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

- Has given a legal opinion on Draft/law "On notification and public consultation";

- Has given a legal opinion on Draft/law "On the Parliamentary oversight of the Intelligent and Security Services ";

- Has given a legal opinion on Draft/law "On asylum";

- Has given a legal opinion on Draft/law "Administrative Procedures Code of the Republic of Albania";

- Has given a legal opinion on Draft/law "On some additions and amendments to the Law No. 8454, dated 04.02.1999 "On Ombudsman";

- Has given a legal opinion on Draft/law "On insurance of the deposits";

- Has given a legal opinion on Draft/law "Service of Internal Control in the Ministry of Internal Affairs";

- Has given a legal opinion on Draft/law "On weapons";

- Has given a legal opinion on Draft/law "On private security service" ;

- Has given a legal opinion on Draft/decision "On the criteria and documentation for entries, residency and treatment of foreigners in the Republic of Albania";

- Has given a legal opinion on Draft/decision "On establishing a Unique System of registration, authentification and identification of users in receiving public services from the electronic systems";

- Has given a legal opinion on Draft/decision on “Procedures of exercise of competencies of the Central Inspectorate and rules for the administration and content of the unique portal “e-Inspection”;

- Has given a legal opinion on Draft/decision of the Council of Ministers “On registration and identification of insured persons, from the compulsory health insurance”;

- Has given a legal opinion on Draft/decision on “Cooperation agreement for the law enforcing agencies, between the Council of Ministers of the Republic of Albania and the Government of the Republic of Turkey”;

- Has given a legal opinion on Draft/decision “On one addition to the decision No. 842, dated 06.12.2006 of the Council of Ministers, “On approval of authorized institutions for electronic verification of the legal status and of the self-declaration form”, as amended”;

- Has given a legal opinion on Draft/decision “On content, procedure and administration of personnel files and of the central personnel register in state administration institutions, private institutions and local government entities”;

- Has given a legal opinion on Draft/agreement of Operational and Strategic Cooperation between the Council of Ministers of the Republic of Albania/ Ministry of Internal Affairs of the Republic of Albania and the European Police Office EUROPOL”;

- Has given a legal opinion on Draft/agreement between the Council of Ministers of the Republic of Albania and the Government of the Republic of Kosovo, for mutual cooperation in the field of security;

- Has given a legal opinion on Manual for Human Rights of internet users, submitted for opinion from the Ministry of Foreign Affairs;

- Has given a legal opinion on the Draft/Agreement of international exchange/transfer sent by the Authority of Financial Supervision;

- Legal interpretation on American Law FATCA (Foreign Account Tax Compliance Act);

- Has given a legal opinion on Draft/Code of broadcasting of the Audiovisual Media Authority;

- Has given a legal opinion on Draft/regulation “On free of charge broadcasting of the messages of higher public interest”.

- Has prepared the Opinion of the Commissioner’s Authority on transparency of publication of the abusing entities data by public institutions;

- Has prepared a Legal Opinion of the Commissioner’s Authority on processing of personal data via internet, either from public and private controllers” (Privacy Policy);

European and International Activities

The participations in events abroad are estimated as very important, with regard to their agendas and to the issues addressed there; the Commissioner’s Authority has been almost an inseparable part of these activities. Along with these very fruitful participations, should be

highlighted the fact that the close cooperation with the Project that assisted our Authority and the results achieved led to:

- KMDP was awarded second prize by the Association of European Projects (EPA) in September 2013 at the European Project Award 2013 in the category "Best Concluded Projects" for the IPA 2009 implemented project;

Institutional participations refer to:

- 7th Conference and 7th General Assembly of the Francophone Association of Personal Data Protection (AFAPDP) 21-22 November 2013, in Marrakesh, Kingdom of Morocco;
- 15th Meeting of the Central and Eastern European Data Protection Authorities, in Belgrade (Serbia), from 10 to 12 April 2013;
- Study visit in Zagreb (Croatia) at the Croatian Personal Data Protection Authority, funded by TAIEX, from 20 to 21 June 2013;
- 35th Conference of the Personal Data Protection and Privacy Commissioners, held in Warsaw, Poland, from 23 to 26 September 2013;
- 25th Case Handling Workshop “On handling practical cases in the field of personal data protection”, held in Sarajevo (Bosnia-Herzegovina), 2-3 October 2013;
- 30th Meeting of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No 108] (T-PD) from 15 to18 October 2013;
- Multi-beneficiary Workshop on data protection auditing with special regard to data protection seals, held in Skopje, FYR Macedonia, 13-14 February 2014;
- Study visit on the Role of Data Protection Officers, in Germany, 14-16 April 2014
- 16th Meeting of the Central and Eastern European Data Protection Authorities, in Skopje (FYR Macedonia), from 1 to 3 April 2014;

The Authority has always aimed to be present and show its consolidation both within the country as well as internationally. In fulfilment of its ends:

- On 28 March 2014, the Authority of the Commissioner for Personal Data Protection became member of the Global Privacy Enforcement Network (GPEN), which in focus of his work has the cooperation of the authorities to achieve and to operate in cooperation for concrete cases or unified standards in the field of personal data protection.

- The International Working Group "On Digital Education".

The Commissioner for Personal Data Protection is a member of the International Working Group "On Digital Education". In this context, the Commissioner has initially completed a questionnaire on the activities organized over the years related to this topic. Later, at the request of the organizers, was sent a fact sheet on the methodology followed by the Commissioner about the organization of the competitions held by the authority of the Commissioner.

Our work and role finalized the acceptance of the application to be already the organizers of an important event and more specifically;

- The Authority of the Commissioner for Personal Data Protection will be the host of the 17th Meeting of the Central and Eastern European Data Protection Authorities, which will take place in 2015;

- In the framework of the EU - IPA 2009.

Monitoring Mission

The Result-Oriented Monitoring Mission, that was carried out by European Commission monitors from 15th to 18th October 2012, two months before the end of the Project awarded the Project "Strengthening of the Data Protection Commissioner Office in Albania for Alignment with European Union Standards" three "As" for "efficiency of implementation", "effectiveness" and "impact prospects" and two "Bs" for "relevance and quality of design" and "potential sustainability".

Contact Persons (Data Protection Officers)

IPA Project activities in particular were related to:

- Drafting of a specialized Training Curriculum for the public sector's data protection officers;
- Implementation of a pilot phase of specialized training for data protection officers, where 38 Data Protection Officers from Ministries and depending Institutions were trained. Also KMDP has trained 22 employers in collaboration with ASPA. In total, number of certified employee in Public Administration reached 60.
- Development of a Practical Guide for the Data Protection Officers.

It is important to note that the contact persons for the protection of personal data have a special role in institutions where they exercise their functions, serving as a bridge between their institutions and KMDP. They follow the issues and inform the Commissioner, require opinions on certain cases and the Commissioner updates with the latest releases and certainly holds frequent connections with them.

Handling of Complaints and Administrative Inspections

The supervisory role over the reporting period (July 2013-April 2014), is successfully implemented by the Commissioner, through the Directorate of Inspection-Investigation, through audits and inspections initiated by complaints of personal data, as well as Administrative Control (ex-officio) pursuant to the Commissioner's Orders.

Complaints

Over the Authority, during this period, are submitted a considerable number of complaints, requests for information and concerns about possible violations (about 55), that were handled by the Directorate of Inspection-Investigation. To the requesting subjects were given the proper legal orientation to exhaust their rights initially at the respective controllers and then be directed to the Commissioner. It resulted that the controllers have fulfilled the legal requirements of the complainants.

For a substantial part of the complaints from various data subjects, was conducted administrative inspection to verify the violation, obtaining the evidences, their examination, drawing of conclusions for violations found, taking measures , and providing responses to the subject/s that have complained.

The object of the complaints reviewed and investigated by the Commissioner has been:

- The accuracy and information on the data processed and obtaining of the consent for direct marketing;
- The publication and disclosure of personal data in the official website of the courts and the media;

- The use and processing of personal data (images) through the use of video-surveillance cameras (CCTV);
- The disclosure of personal data from several public institutions;
- The use and processing of biometric data (fingerprint);
- Respect for the right of access and rectification, for the personal data of data subjects;
- The publication of personal data of complainants in the portal of the Ministry of Justice (Denounce Corruption).

Administrative Control and inspections (ex-officio) pursuant to the Commissioner's Orders.

Pursuant to its supervisory policy, for this period the Commissioner exercised administrative controls and inspections in 184 different controllers (about 37 more than in the previous report). This activity is extended in some districts, such as Tirana, Durrës, Shkodra, Vlora, Fier, Korca, Peshkopi, Lezha, Saranda, Gjirokastra, etc. The aim of supervision tasks for this period has been the increase of the number of supervisory activities and expansion of the control into new fields of the processing of personal data. The findings obtained in the particular controllers, served to perform risk analysis for the relevant field, by the intervention of the Authority, realized through various acts (instructions, recommendations, orders, opinions, etc.), which have served to all controllers of the area (courts, education, health, etc.). Areas where administrative control is exercised are:

- Banking system;
- Public and private healthcare system;
- Central state institutions;
- Public service institutions;
- Law enforcement institutions (police, courts);
- Free professions (notary, lawyer) ;
- Written and audiovisual media;
- Electronic communications.

These controls are focused on the processing of personal data by big data controllers. The objects of these controls were thematic and aimed to monitor and supervise the processing based on the law and Commissioner's specific acts, according to the fields. So in this context have been inspected several important public controller, such as the Ministry of Justice, Court, Healthcare Insurance Institute, General Directorate of Customs, the Ombudsman, the General Directorate of Metrology, University Hospital Center etc.

There were performed controls in several private controllers in order to verify the processing, obtaining of the consent, the international transfer of personal data, data processing in the surveys, development of direct marketing, publishing statistics in the media, as well as to verify the fulfillment of the obligation to notify. Regarding the obligation to notify is followed a strategy that, if the controller within 48 hours of initiation of inspection fulfill this obligation shall not be taken administrative measures with fine. This practice has worked and in most of the cases the subject has notified and only in one case is applied the fine.

For all the violations found during administrative controls, the Commissioner has come up with the final acts, in order to terminate the violation, creating legal space by the controller to ensure data protection, compliance of the processing operations with the principles of the laws and Commissioner acts.

Fines

Pursuant to the competences of the Commissioner, after the closure of the inspection procedures and administrative controls, are decided seven penalties for entities belonging to the field of journalism and media (2) regarding the disclosure of personal data without their anonymisation and the deleting upon completion of the purpose, health area (1) associated with the data collected disproportionately towards the purpose and not obtaining the consent, big business (4) associated with non-compliance with the duty to inform the subjects in the case of consent were exercise direct marketing, drafting acts that guarantee security and confidentiality, the international transfer in a country without an adequate level of protection of personal data without the consent of the data subjects without meeting the legal criteria, non-compliance with the terms of the retention of personal data, non-compliance with the measures for physical and technical security of personal data and for non-compliance with the duty to notify.

We note that, as opposed to the increased number of administrative controls and inspections, the number of fine decisions is lower from the previous reporting period, this for the primary reason that has resulted and is observed the immediate action by the controllers, ceasing violations found, which is the goal, the strategy and policy of the Authority. Only in repeated cases of violation, not taking action after issuing orders and recommendations and ongoing violations of the rights of individuals, the authority has seen the inevitable imposition of fines.

Fulfilment of the important obligation of the data controllers and execution of the notification in the processing of personal data of the individuals is one of the priorities of our institution.

In this context as a first and estimated step with expectation is the intensive continuation of the process of sensitization of the data controllers in the implementation of the cooperation agreement concluded between the Commissioner for Personal Data Protection (CPDP) and National Registration Center (NRC). In this regard the Registration Department has sent about 1192 official awareness raising letters addressed to data controllers. The total numbers of these letters, including both private and public sector is 17556.

Also, another way of sensitization with positive results was also sending e-mails to many important data controllers such as to the Pharmacies. In this regard 773 sensitization e-mails were sent.

We have signed a cooperation agreement with the National Employment Service, in order to sensitize the data controllers, pursuant which the physical and electronic list of subjects that the NES holds, was provided to us. In the framework of the electronic correspondence, 327 sensitization e-mails were sent.

One among our priorities was the assistance given to the data controllers that notified, in order to help them to complete the notification form in the correct way. This assistance was offered through electronic communications (about 650 assistances), e-mails (about 80 clarifications via e-mails), and also engaging in front desk help the representatives of these data controllers in the Office of the Commissioner (about 145 meetings).

Also, within the implementation of the cooperation agreement signed by the Ministry of Education and Science and our Institution, our work during this period continued with activities in the education sector too. In this way, we had meetings in the Education Department of Berat, Lezhe, Permet and also with the Education Department of the District Council of Tirana.

Management of notifications and registration of data controllers.

We have reviewed the notifications, the requests for supplementary information; additional information provided by data controllers, alteration declarations and also official notes replies.
The number of notifications received from data controllers in this period was 650, of which 49 were nonprofit organizations, 122 were public subjects and 389 private subjects. The total number of notifications reached 4262.

The number of controllers registered in this period is 566, of which 48 are nonprofit organizations, 121 are public subjects and 397 private subjects. The total number of notifications reached 4208.

Awareness - raising

The Commissioner for Personal Data Protection has continued the awareness raising activities of data controllers and data subjects with special focus on the youth, due to the rapid development of advanced technology and the rapid processing of personal data in social networks. In this context, the activities are carried out as follows:

- The Commissioner has published two new leaflets which are mainly dedicated on Smartphone and concrete examples of misuse of personal data in social networks.

- During this year the Commissioner has undertaken a new initiative which is the publication of the legal magazine "Law and Privacy". This is a 6 monthly periodical magazine of the Commissioner's Authority. The first two numbers of the magazine has seen published articles related to the field of personal data protection from domestic and foreign experts.

- On the occasion of the Convention on the Rights of the Child, on 20.11.2013, the Authority of the Commissioner held a meeting with the students of "Faik Konica" school. The purpose of the meeting was: "Sensitizing the children concerning the risks on privacy that may be caused by the dissemination of personal information on the Internet". During this meeting, a presentation was held with special regard to this age group. This presentation grabbed the attention due to the fact that almost all participants in the meeting own profiles in social networks. Leaflets were distributed to the students and teachers attending the meeting.

- On the occasion of the celebration of January 28th - Data Protection Day, The Commissioner for Personal Data Protection organized the conference on "The Protection of Personal Data, a fundamental human right" with the participation of representatives of civil society. The welcoming speech was held by Mrs. Flora Çabej (Pogaçe), the Commissioner for Personal Data Protection. In her speech Mrs. Çabej highlighted the key areas where personal data is affected. The conference continued with the presentations of the General Secretary of the Albanian Assembly; the Ambassador of the EU Delegation in Albania, Deputy Ambassador of the OSCE Presence in Albania and the Head of the Council of Europe. The second part of the conference was addressed by Albanian and European experts on important issues of personal data protection.

- In parallel with the conference, the Commissioner for Personal Data Protection s ran "Open Day" at the Authority. Representatives of the Authority from 11:30 to 12:30 am were the citizens by answering every question and complaint on privacy related issues.

- On the eve of January 28, at the "Dora d'Istria" School was organized the contest: "Protecting privacy". Many students submitted their literary creations in Albanian, English and French languages and a joint jury of teachers and representatives of the Commissioner

distributed awarding certificates for the best papers. Also a representative of the Commissioner explained to the students the risks arising from neglecting the protection of privacy in communications within the social networks.

- On the day of signing of the cooperation agreement with UNYT, on January 2014 the Commissioner Mrs. Çabej Pogaçe delivered a public speech during the meeting with students on the topic "New Dimensions in Privacy Law" speaking about the law enforcement and the most recent changes, through concrete examples and solutions to complaints that the Commissioner's Authority has provided.

- This meeting was followed in February by a second meeting among the Commissioner's authority representatives and Master level students of the University, whom were informed more closely on the Commissioner's activity in the implementation of the Law on Personal Data Protection.

- On 3/12/2014 representatives of the Commissioner held a training seminar for employees of the General Directorate of State Police with regard to the law on protection of personal data but mainly on its amendments, its innovations and also concerning other significant topics.

- The Commissioner for Personal Data Protection to be closer to technological change and innovation required has launched a new website which is visually improved and more interactive and attractive to the public.

Media

Media relations are intensified in this period as a result of greater public interest about the right of protection of personal data.

In this time period two media conferences were organized and several interviews by the Commissioner for the Protection of Data Personal or other representatives of the Commissioner which were mostly broadcasted in news programs but also in other national television programs. The Commissioner Authority was invited from the National TV to take part in three talk-shows concerning the right for personal data protection.

During this period of time, the Commissioner for Personal Data Protection has sent in two cases, written recommendations to press media regarding publication of the identity of victims of violence, especially when it comes to minors in order not to have a second victimization of people involved in a crime event as long as there is a right of presumption of innocence.

In order to increase reporter's sensitivity about this topic, in March of 2014 the Commissioner invited in a meeting, representatives of the journalists' association. In the center of the discussions the ethic in the media and the respect for private life, with regards to the publication of personal data of minors victims of violence or extreme exposure of the private life of the story's characters goes beyond what is the public interest information and crosses the boundaries of ethical and moral norms.

ANDORRA / ANDORRE

Développements majeurs intervenus dans le domaine de la protection des données à Andorre depuis la 30ème réunion plénière du T-PD (15-18 octobre 2013) :

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

La Loi 18/2013, du 10 octobre, de modification du Code pénal. Cette loi a apporté certaines modifications à la Loi 9/2005, du 21 février, au sujet principalement du blanchissement de capitaux, le délit d'initié et l'information privilégiée, contre la confidentialité à travers des systèmes informatiques et la production, la vente, la diffusion ou d'autres formes de mise à disposition d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à l'ensemble ou à une partie d'un système informatique.

Le Règlement du 19 février 2014 qui fixe les conditions de fonctionnement du Service d'Immigration ainsi que le Registre Central de l'Immigration. Les articles 10, 11 et 12 règle les données que doit contenir le Registre ainsi que les communications et les droits d'accés et rectification.
Le Règlement du 17 octobre 2012 qui réglait le Service d'Immigration est abrogé.

Le Règlement du 11 décembre 2013 sur le passeport ordinaire établit les caractéristiques du passeport biométrique et les données personnelles qu'il doit contenir.

REPUBLIK ÖSTERREICH
DATENSCHUTZBEHÖRDE

Sachbearbeiter: Dr. Matthias SCHMIDL

Major developments in the data protection field in Austria

In response to your e-mail of 2 May 2014, the *Datenschutzbehörde* (Austrian DPA) submits the following facts:

1. As of 1 January 2014 the *Datenschutzkommission* was replaced by the *Datenschutzbehörde* as the Austrian DPA. Just like the *Datenschutzkommission* the *Datenschutzbehörde* fulfils all requirements of Art. 1 of the Additional Protocol to Convention 108 and of Art. 28 of Directive 95/46/EC. The replacement is a consequence of the establishment of Administrative Courts which will deal with appeals against decisions of administrative authorities. A decision of the *Datenschutzbehörde* is now subject to judicial review by the *Bundesverwaltungsgericht* (Federal Administrative Court) and then of the *Verwaltungsgerichtshof* (High Administrative Court) and the *Verfassungsgerichtshof* (Constitutional Court).

Ms Andrea Jelinek was appointed Head of the *Datenschutzbehörde* for a term of five years. *Mr Matthias Schmidl* was appointed Deputy Head for the same term.

The relevant amendment of the Austrian Data Protection Act 2000 was published in Bundesgesetzblatt I Nr. 83/2014 and entered into force on 1 January 2014.

Further information about the *Datenschutzbehörde* is available at www.dsb.gv.at.

2. The former *Datenschutzkommission* decided on 18 January 2013 to submit to the EJC several questions concerning the interpretation of the Data Retention Directive 2006/24/EC for a preliminary ruling (Case C-46/13).

Since the Data Retention Directive was annulled by the EJC in its judgment of 8 April 2014, joint cases C-293/12 and C-594/12, the *Datenschutzbehörde* decided to withdraw the request.

6. Mai 2014
Für die Leiterin der Datenschutzbehörde:
SCHMIDL

BELGIUM / BELGIQUE

Conseil de l'Europe – Réunion plénière du T-PD de juin 2014

Principaux développements intervenus au niveau national depuis la dernière réunion plénière

---

1. ***Modifications de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Loi « Vie privée »)***

- ✓ Suspension (sous conditions) du droit d'accès lors de contrôle et enquête fiscale par le ministère des Finances

L'article 3 de la Loi vie privée – qui, pour certains traitements de données identifiés, prévoit un régime dérogatoire – prévoyait depuis 2012, entre autres dérogations, une suspension du droit d'accès aux données relatives aux traitements gérés par le Service public fédéral (ministère des) Finances durant la période pendant laquelle la personne concernée est l'objet d'un contrôle ou d'une enquête ou d'actes préparatoires à ceux-ci .

Jugé inacceptable par la Commission de la protection de la vie privée notamment[1], une modification de cet article est intervenue en 2013. Il y est désormais prévu que le droit d'accès est certes suspendu pendant les circonstances précitées, *mais uniquement dans la mesure où la mise en œuvre de ce droit d'accès nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires* ***et*** *pour leur seule durée*. La durée de ces actes préparatoires pendant laquelle le droit d'accès n'est pas applicable, *ne peut excéder un an à partir de la demande d'accès*.

L'exception est par ailleurs immédiatement levée après la clôture du contrôle ou de l'enquête ou dès la clôture des actes préparatoires lorsque ceux-ci n'ont pas abouti à un contrôle ou une enquête. Le Service de Sécurité de l'Information et Protection de la Vie Privée (organe de contrôle interne) créé au sein du Service public fédéral Finances en informe le contribuable concerné sans délai et lui communique dans son entièreté *la motivation* contenue dans la décision du responsable du traitement ayant fait usage de l'exception.

Pendant cette période de suspension du droit d'accès aux conditions ci-dessus, la personne concernée dispose d'un droit d'accès indirect – comme en matière policière – qu'elle exerce par l'intermédiaire de la Commission de la protection de la vie privée (article 13 de la Loi Vie privée).

- ✓ Création d'un Organe de contrôle de la gestion de l'information policière au sein de l'autorité de protection des données(loi du 18 mars 2014)

La loi du 18 mars 2014 crée auprès de la Commission pour la protection de la vie privée un Organe de contrôle de l'information policière chargé du contrôle du traitement des informations et des données visées par la loi relative à la fonction de police. Dans l'exercice de ses missions, cet Organe est indépendant de la Commission de la protection de la vie privée dont il partage toutefois le secrétariat. Essentiellement composé de membres des polices fédérale et locale

---

[1]Commission de la protection de la vie privée, Avis 32/2012 du 17 octobre 2012. (http://www.privacycommission.be) Dans un arrêt du 25 mars 2014, la Cour constitutionnelle de Belgique, saisie d'une demande d'annulation de la modification initiale (avant révision en 2013) annule cette disposition.

ainsi que d'experts, l'organe doit compter un commissaire de l'autorité de contrôle (Commission de la protection de la vie privée) parmi ses membres.

L'Organe de contrôle est particulièrement chargé de contrôler le respect des règles d'accès direct à la B.N.G. (banque nationale de données policières) et d'interrogation directe de celle-ci, ainsi que de contrôler le respect par l'ensemble des membres des services de police de l'obligation, d'alimenter cette banque de données. Il veille, par le biais d'enquêtes de fonctionnement, à ce que le contenu de la B.N.G. et la procédure de traitement des données et informations, qui y sont conservées, soient conformes aux règles prescrites par la loi sur la fonction de police et à leurs mesures d'exécution, en particulier la régularité des opérations de traitement telles que la saisie des données et informations enregistrées en fonction du caractère concret ou de la fiabilité de celles-ci ou encore l'effacement et l'archivage des données et informations à l'échéance de leurs délais de conservation. Les banques de données particulières (à durée limitée dans le temps par exemple), font également l'objet d'un contrôle. L'organe dispose de pouvoirs d'enquête et rapporte, ponctuellement et/ou annuellement, à la Chambre des représentants.

2. *Vers une modification des articles 3 et 9 (droit à l'information) de la Loi Vie privé ? Affaire Institut des professionnels de l'immobilier c. Englebert et autres portée devant la Cour constitutionnelle belge et la Cour de Justice de l'Union européenne*

L'affaire visait à savoir si la loi belge, en ne prévoyant pas d'exceptions pour les détectives privés comparables à celles visées à l'article 13, paragraphe 1, sous d) et g), de la directive 95/46, transpose correctement cette disposition. En effet, en ne prévoyant pas d'exception particulière pour les détectives privés, l'obligation d'information leur est applicable. La question se posait alors de savoir si d'une part il y avait une inégalité de traitement dans le chef des détectives privés et d'autre part si l'exercice de la profession de détective privé était encore possible dans ces conditions. En Belgique, la profession de détective privé est réglementée par une loi du 19.07.1991.

Saisi en 2012, le Tribunal du commerce a, au vu des questions qui se posaient, interrogé la Cour constitutionnelle belge. La Cour Constitutionnelle belge a, quant à elle, interrogé la CJUE.

La CJUE a rendu son arrêt le 7 novembre 2013 (C-473/12) http://curia.europa.eu/juris/document/document.jsf?text=&docid=144217&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=182002 et la Cour constitutionnelle belge a rendu son arrêt le 3 avril 2014. http://www.const-court.be/public/f/2014/2014-059f.pdf

La Cour constitutionnelle belge a jugé que la disposition en cause de la loi « vie privée » belge du 8 décembre 1992 viole les articles 10 (principe d'égalité) et 11 (principe de non-discrimination) de la Constitution belge dans la mesure où l'obligation d'information s'applique automatiquement à l'activité d'un détective privé ayant été autorisé à exercer ses activités pour des personnes de droit public conformément à l'article 13 de la loi du 19 juillet 1991 « organisant la profession de détective privé » et agissant pour un organisme professionnel de droit public (Institut des professionnels de l'immobilier) qui est chargé par la loi de rechercher des manquements à la déontologie d'une profession réglementée (agents immobiliers).

3. *Modification de la Loi relative aux communications électroniques – nouvelle compétence pour la Commission de la protection de la ,vie privée en matière de data breach*

Depuis avril 2014, c'est *la Commission de la protection de la vie privée* , et non plus l'Institut belge pour les télécommunications, que les entreprises fournissant des services de communications électroniques accessibles au public doivent avertir en cas de violations de données. La Commission avertira elle-même l'Institut. La Commission est également tenue de veiller au respect par ces entreprises de la notification de la violation aux particuliers lorsque celle-ci s'impose. Un partenariat entre l'Institut belge des télécommunications et la Commission de la protection de la vie privée intervient par la suite.

4. *Modification du paysage institutionnel de la protection des données*

Aux côtés de la Vlaamse toezichtcommissie (commission de contrôle de l'échange des données entre administrations flamandes dans le cadre de l'administration électronique), une commission de contrôle des échanges de données au niveau régional wallon et bruxellois ont été créées.

5. *Activités de l'autorité de protection des données*

Le rapport annuel de la Commission de la protection de la vie privée détaille l'ensemble de ses activités. Quelques-unes méritent une attention particulière http://www.privacycommission.be :

- **Sensibilisation des mineurs** : la Commission belge de la protection de la vie privée a initié la mise sur pied d'une pièce de théâtre comique et éducative sur le thème de la protection des données (activités en ligne et vie privée) s'adressant aux élèves de l'enseignement primaire (en néerlandais uniquement). Elle a élaboré un kit pédagogique complet « Je suis jeune et je protège ma vie privée » dont un volet prend appui sur la pièce de théâtre précitée. Voir le site spécifique http://www.jeddecide.be et http://www.ikbeslis.be

- **Violations de données – data breach :** A la suite de plusieurs fuites importantes de données (dont la copie d'un fichier de la clientèle de la sociétés de chemins de fer belge concernant 1,4 million de personnes), la Commission belge de la protection de la vie privée a élaboré un certain nombre de recommandations destinées à prévenir de telles fuites, le plus souvent dues à une sécurisation insuffisante des données traitées.

- **Travaux sur le projet de règlement UE (EU data protection reform)**: la CPVP a rendu deux avis importants dans le contexte de la réforme de la protection des données négociée au sein de l'Union européenne. Son avis 35/2012 porte sur la proposition de règlement initialement déposée par la Commission européenne alors que son avis 10/2014 porte sur le texte voté par la Commission LIBE en octobre 2013.

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

PDP development in 2013

The Office for Personal Data Protection Czech Republic

I.

LEGISLATIVE ACTIVITIES

In 2013, a new key area of work in the field of legislation was the Data Protection Impact Assessment ("DPIA"), introduced into the legislative rules of the government in 2012. After many years of bustling legislative activity, which often did not take into account the specifics of work with information and privacy protection to a great degree, an instrument finally appeared in the Czech Republic, in the form of the DPIA, that reminds the people in charge of drafting regulations that they need to focus on implementing privacy protection rules already at the time of drafting plans and concepts, i.e., not by general proclamations about data protection with reference to Act No. 101/2000 Coll., but by describing and assessing the specific impacts of the proposed legislative solutions in existing and planned areas of personal data processing.

As part of the consultation procedure in respect of draft legislation, the Office attempted, in those cases where documents were presented to it, to identify key aspects of the intended personal data processing and propose the approach to take when drawing up DPIA, i.e., the obligation to explicitly state whether the proposed wording establishes a new personal data processing requirement, and if so, to justify the need for it and to describe its basic parameters: the purpose of processing, the category of processed personal data and key parts of the processing, namely the outputs of the processing and the personal data retention periods, with specifics and rules for publishing and accessing data on the Internet, which is so popular at this time.

With regard to the DPIA, it is not possible to accept draft legislation corresponding to information systems that were not set up in compliance with the principles for working with information and privacy protection (Privacy by Design).

The Office called attention to the need to draw up DPIA especially in the case of registries (registers, records) with personal data, which are kept by the public authorities. The legal regulation on maintaining registries is often very unspecific. Laws often contain only general mandates on maintaining registries, with the issue being delegated to implementing regulations, decrees or even the internal regulations of the registry administrator, which are usually not open to data subjects. Only to a limited degree is it possible to refer to the new Act on Public Registers of Legal Entities and Individuals, which pertains to a number of specific databases. According to the case law of the Constitutional Court (e.g., Ruling No. Pl.ÚS 24/10 dated 22 March 2011 or Ruling No. Pl. ÚS 24/11 dated 20 December 2011) as well as of the European Court of Human Rights (e.g., Leander v. Sweden of 26 March 1987 or Amann v. Switzerland of 16 February 2000), the collection and retention of personal data is already an infringement of the basic right to privacy, with it not being decisive whether their further processing takes place or not. Personal data collection in registries kept by the state administration or local or regional government, as a rule with the consent of the individual concerned, is thus infringement of the right to privacy. The rules for such infringement should then be sufficiently regulated in the law.

In 2013, in matters regarding registries, the Office, in the framework consultation procedure, provided guidelines for the drafting of legislation concerning a specific registry and required that the submitter of the bill always made it clear whether the proposed registry would be open to the public or not. The Office also often recommended that the registry be divided into a public and non-public part, along with specification of which information will be freely accessible. At the same time, it called attention to the obligation to clearly express the purpose for which the personal data should be made accessible and to the obligation to stipulate rules that ensure that the data are not presented in an inaccurate our outdated form. An example of a proposed improvement to a registry includes the requirements that the Office addressed to Ministry of Industry and Trade regarding the Trade Licencing Register. The Office proposed a more exact division of this register into a public and non-public part. The Office recommended placing restrictions on the publication of data that pertain more to the privacy of the entrepreneur than to his/her business activities – in cases where the businessperson states a business address that is different from his/her residential address, the residential address need not be made available in the public part of the register; furthermore, should the business address and residential address coincide, it is not necessary to state that the business address is in fact the same as the residential address.

In 2013, the Ministry of Health repeatedly called attention to the fact that the provisions of the Health Services Act were not duly substantiated and in the form approved do not provide an explicit guarantee that the processing of personal data will be in line with the law – the provisions are not even linked to the basic obligations set out in Act No. 101/2000 Coll. (in particular: the exactly defined purpose of processing, the proper legal reason for using the personal data, and the substantiated reasonable retention period). Without more specific rules, more doubts can be raised about the purpose and effectiveness of the entire NHIS and the transparency and credibility of the output from it.

In connection with its participation in public discussion on the draft Cybernetic Security Act, the Office was able to advance its comments calling attention to the fact that a necessary statutory condition for disposing of records according to this legislation will be the maintenance of electronic records in a way that will allow one to determine and verify when, by whom and for what reason data collected under this legislation was processed, including for how long and for what purpose they were retained (not excluding destruction protocols). The documentation on processing data used in the fight against cybercrime considers the personal data protection measures set out in Article 13 of Act No. 101/2000 Coll., which create the conditions for any required supervision and enforcement of the statutory obligation to maintain confidentiality, to be effective and technologically adequate.

As part of measures connected to the adoption of the Inspection Code, which the Office will begin to observe as of the beginning of the year, the draft Personal Data Protection Act was finalised and presented to Parliament for passage. With regard to the new assignment from the government to deal collectively only with issues that directly pertain to the Inspection Code, the most ambition part regarding the status of the board of inspectors was deleted from the new version of the bill. The procedure to be taken by inspectors as part of the board (e.g., discussion of objections against the inspection protocol) will thus be regulated, as was the case in the past, by the internal regulations of the Office.

With respect to one of the highest political priorities of the Czech Republic, i.e., implementation of a public service system, the persons responsible for drafting the respective legislation took into account the position of independent administrative bodies, of which the Office is one.

II.

FINDINGS FROM COURT REVIEWS

Numerous decisions of the Office are subject to court review. As regards specific findings from the relevant court rulings in 2013, it is possible to call attention to a number of important decisions regarding the operation of camera surveillance systems and the publication of personal data in particular.

Surveillance using video cameras, where recordings are made and then the individuals who are recorded are identified in those cases determined by the personal data administration, is deemed the processing of personal data, even in those cases where the recorded individuals are not identifiable in practice.

In the opinion of the Supreme Administrative Court, personal data is collected and processed even in situations where no additional information is provided with the only identifier, i.e., the face; nevertheless, it is possible to subsequently identify the person (from the date when a seminar or meeting took place, who organised it, the list of participants etc.). Furthermore, it can also be deduced that the purpose of the recording – protection of interests protected by law – assumes that such identification can be expected.

A local or regional government with an established police force is not authorised to set up a camera surveillance system that would likely not be permitted if it were a private entity; in this connection, it cannot be argued that the municipal police is part of the local or regional government in question when the camera surveillance system was in fact not installed for the police force.

According to the mentioned ruling, although the municipal police may not be an independent legal personality and the respective municipality is bound by the legal acts of the municipal police, it is necessary to call attention to the fact that in the assessed matter it is not decisive who has or does not have legal personality, but what the respective legal regime is and what purpose the camera surveillance system is in fact set up for.

The disclosure of personal data of those persons who contacted the municipality with their instigations or requests has to be based on a legal reason that cannot be derived just from the specific act of filing.

The Municipal Court in Prague ruled that the disclosure of personal data on the website of a municipality is not necessary for the handling of the requests, i.e., for fulfilling the purpose for which the personal data was collected. A request as such is not consent to disclosure of the personal data contained therein on the official bulletin board or website; it can only be understood as consent to process the personal data as part of request handling procedure

III.

RAISING AWARENESS on PDP

Information bulletin

As part of the annual “My Privacy! Don’t Look, Don’t Snoop!” contest, we tried to ask young people whether they know how to make use of privacy protection possibilities offered to them on the most personal data hungry network: Facebook. The responses that we received we are adding to the special issue of the Information Bulletin as an inspiration: The Bulletin devoted mainly to teachers, parents are not precluded.

The Buletin was distributed with the Student Diary to 8 000 schools. The contributions that we have included in the 2013/2014 Student Diary “Good Advice is More Valuable than Gold! How to Protect Your Privacy on Facebook” may help with this.

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

GEORGIA / GEORGIE

OFFICE OF THE PERSONAL DATA PROTECTION INSPECTOR

Information on Major Developments

October 2013 - May, 2014

Data Protection Supervisory Authority – Formation of the Office

The formation of the Office of the Personal Data Protection Inspector of Georgia is already complete. There are 2 main departments: (i) **Citizens' Complains and Inspections Department** *(the main objective of the Department is to deal with citizens' complaints on the personal data protection related issues, to investigate the lawfulness of the data processing by public and private institutions and provide consultations to the data controllers, data processors and data subjects)*; and (ii) **International Relations and Communications Department** *(the main objective of the Department is to cooperate with different international organizations, to define public and media communications strategy, to conduct educational activities and to raise public awareness on privacy and personal data protection related issues)*.

Annual Report on the State of Data Protection in the Country

The Personal Data Protection Inspector submitted to the Government of Georgia the first **Annual Report on the State of Data Protection in the Country** on March 1, 2014. The Report was publicized on the web-page of the Office and presented to public and mass-media representatives as well. Annual Report analyzes the current situation in terms of data protection on the basis of the citizens' complaints, conducted inspections and held consultations and summarizes the respective findings. Report covers all important issues related to the personal data protection in Georgia, *inter alia,* practice of applying basic principles of data protection, legal grounds for data processing, processing of biometric data, conducting video surveillance, direct marketing, etc. In addition, the Report provides for the recommendations to the Government in order to ensure high level of personal data protection in the country.

Web-Page of the Data Protection Supervisory Authority

The web-page of the Office of the Personal Data Protection - www.personaldata.ge; www.pdp.ge - was officially launched on Data Protection Day, January 28, 2014.

The web-page provides for the information on the structure, staff, basic activities and budget of the Inspector's Office. Publications, statements of the Inspector, national legislation and international acts on data protection are available on the web-page. The main content of the web-page has a user friendly design and is divided into 3 major blocks – (i) **For Individuals**; (ii) **For Private Organisations**; and (iii) **For Public Organisations**. These units display the detailed information for the respective addressees, such as rights of the data subjects and

scheme on the realization of these rights, obligations of data controllers, online privacy, data security related issues, etc.

Legislative Developments

In November 2013 the Office of the Inspector launched the process of elaboration of legal amendments to the PDP Law and other normative acts since there is a need to harmonize the national legislation with best European and international standards such as CoE 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. A special Working Group, comprising representatives of the Parliament, Ministry of Justice, Ministry of Internal Affairs, State Chancellery and non-governmental organizations, was created with initiative of the Personal Data Protection Inspector. The Working Group finalized the text of the draft amendments and they were submitted to the Government of Georgia for initiation in the Parliament in May 2014. The Government discussed the Amendments and decided to initiate them in the Parliament. The Government also decided to incorporate the extension of the Inspector's mandate towards data processing in police sector (in line with *CoE Committee of Minister's Recommendation (87) 15*) therein.

Under the draft amendments the range of sensitive data will be enlarged and genetic data, also data related to the all type of criminal records, administrative liabilities and recognition of a person as a victim of a crime will be added. Provisions related to direct marketing will be enhanced and regulations on video surveillance in public transportation means will be added as well. Amendments also foresee the election and appointment of the Inspector by the Parliament and accountability of the Inspector towards the Parliament. Amendments enhance the financial guarantees of the Inspector's Office and inviolability of the Inspector. In addition, Amendments provide for the full enactment of Law on Personal Data Protection in 2014 instead of 2016 and increased sanctions for some significant violations of the Law on Personal Data Protection.

Guidelines and Recommendations

The special forms to be filled out by the data controllers on *trans-border data flows*, *processing of biometric data* and providing *notification on filing systems catalogues* have been elaborated by the end of December 2013. These forms are accompanied by the specific guidelines providing detailed rules on filing out the forms.

In April 2014 the Office launched the process of elaboration of sector specific and thematic recommendations, *inter alia,* on data processing for employment purposes, data processing in insurance sector, data processing for the purposes of direct marketing, data disclosure by public bodies, data processing in telecommunications sector, processing of medical data. The Recommendations will be based on the CoE Committee of Ministers Recommendations on respective issues *(such as Recommendation No. R(2002)9 on the Protection of Personal Data Collected and Processed for Insurance Purposes; Recommendation No. R(89)2 on the Protection of Personal Data Used for Employment Purposes; Recommendation No. R(99)5 on the Protection of Personal Data on the Internet; Recommendation CM/Rec (2010) 13 on the Protection of Individuals with regard to Automatic Processing of Personal Data in the Context of Profiling)*. According to the schedule, the Recommendations will be issued throughout June-December 2014.

Education and Public Awareness Raising

One of the main directions of the Office of the Personal Data Protection Inspectors is to raise public awareness and to conduct educational activities on personal data protection related issues. The Office fruitfully cooperates with the number of public bodies. The Memorandums of Understanding were signed with the Training Center of Justice and Academy of the Ministry of the Internal Affairs. Within the scope of the MOUs numerous trainings were conducted. In February 2014 trainings were held for the employees of the Ministry of Internal Affairs; in March 2014 training of the employees of the National Archive of Georgia took place. Furthermore, Personal Data Protection is incorporated in the Labour Code and Administrative Code training course conducted within the Training Center of Justice. Specific training on Personal Data Protection in Consular Relations was delivered to the employees of Ministry of Foreign Affairs in cooperation with the Training Center of the Ministry. Personal Data Protection Trainings cover issues such as principles of data processing, legitimacy of data processing, databases, video surveillance, processing of biometric data and etc.

Data Protection Day

On January 28 the Office organized a *special event dedicated to the Data Protection Day. Aim of the event was to bring to the attention of the public the importance of the right to privacy and provide forum for discussing proposals on consolidating national legal framework in terms of data protection regulations and harmonizing legislation with European and international standards. More than 100 participants from public and private institutions, corps diplomatique, international and non-governmental organizations attended the Event.*

Special State Commission on Illegal Surveillance Materials

The Inspector was actively involved in the work of the Special State Commission dealing with Illegal Surveillance Materials stored at the Ministry of Internal Affairs. As a result of the work done by the Commission, initially the materials (110 CDs containing 181.32 minutes of illegal recordings of the highly sensitive intimate scenes) were publicly destroyed. According to the Decision of the Commission (29.01.2014) from the rest of the materials (635 CDs in total, containing 382 Gigabytes of 750 hours recordings) only several CDs containing highly sensitive intimate scenes were destroyed, while others depicting less sensitive information (e.g. conversations of businessmen, politicians, etc.) were submitted to the prosecution services for investigative purposes.

Statistical Data

According to the statistical data, since July 2013 The Office provided **503** verbal and **48** written consultations; discussed **18** citizen's complaints; conducted **2** inspections; issued **1** authorization on transborder data flow; trained **409** public officials and other interested persons on personal data protection related issues.

Country report
HUNGARY

The National Authority for Data Protection and Freedom of Information (hereinafter: NAIH) started its operation in January 2012. The new institution was granted more powers. The most important innovation, in line with the spirit of Directive 95/46/EC, was that besides becoming a separate entity from the general Ombudsman's institution, it was granted administrative sanction powers, and thus can also impose fines on controllers who harshly violate data protection rules. The NAIH has used these new powers each time it deemed it necessary. Last year, 36 new data protection cases were conducted within an administrative procedure, and 31 fines imposed. Some of these decisions were appealed by the data controllers, and this is going to lead to a new case law in Hungary, that was lacking up to this day, on data protection. It is an encouraging signal to us that the courts have upheld the vast majority of our decisions they examined (6 out of 8).

A major event that recently reached the NAIH was the European Court of Justice's (hereinafter: ECJ) decision establishing Hungary's infringement to article 28 of Directive 95/46/EC. This decision, however, has no impact on the NAIH's decisions and its overall functioning.

The ground-breaking invalidation of Directive 2006/24/EC on Data Retention, on the other hand, can have a serious impact on data protection EU-wide. It may have serious repercussions on data protection in the field of telecommunication services and the protection of meta-data. At present time, the analysis of the legal consequences on Hungarian law is still ongoing. More generally, the NAIH is also working with its international partners on adopting its strategy on cell data and meta-data regulation.

Since 2012, according to its legal duties, the NAIH organises twice a year a national Conference of Internal Data Protection Officers. If the new Regulation is adopted, DPO's will become a new cornerstone of data protection. This is a new trend in Hungary, and we are watching closely how our international partners work with DPO's in order to implement the best practices.

Processing operations by websites have been one of our major concerns. Our investigations have shown that especially children's rights were often violated in an on-line environment. This led to the launch of a long-term study project on children's rights in an on-line environment, that will be presented at the end of this report.

The use of biometric systems is increasing in Hungary as in the rest of Europe. During data protection audits as well as investigation procedures, the NAIH has enforced its opinion, based on the Article 29 Working Party's opinion, that the use of these systems must respect the principle of purpose limitation and proportionality. One of the cases that we examined will be developed later in this report.

Marketing is one of the industrial sectors that make the most use out of personal data. On the long term, the NAIH wishes to improve its supervision on marketing databases. This work was started last year by an investigation that led to a financial sanction, detailed later on in this report.

Finally, data security is a major concern as well. Even when data controllers take serious protection measures, breaches can happen. But many do not comply with the minimal legal requirements on data security. One such case is also detailed in this report.

Relevant case, 2013

a) Investigations into data processing operations by websites, registration processes, the enforcement of data subjects' rights on the Internet, and especially those of children

NAIH undertook an overall investigation of data processing operations by certain websites, where we wanted to evaluate the privacy policies, the registration processes, the scope of processed data, and the enforcement of data subjects' rights. In the frame of this procedure, the NAIH gave special attention to the processing of children's data. The importance placed on minors as data subjects during our procedure was justified by the fact that, contrary to the former Data Protection Act, the new Privacy Act, in its article 6 paragraph 3, provides that children over 16 have the right to consent to data processing operations independently from their legal guardians.

The NAIH encountered the case of a company operating several types of websites, including dating websites where it was usual to find registered users under the age of 16, who were able to register despite the absence of their guardians' either prior or subsequent consent. NAIH investigated several dating websites and observed that minors below 16 could frequently be found as registered users. According to the NAIH, it is important to place the child's superior interests into highlighted account when examining their online activities and the data processing operations that concern them. This is particularly true in the case of social networks. Inside this category, dating websites represent the greatest threat. Indeed, unlike regular social networks where users communicate mostly with known friends, the main function of dating websites is to meet new people. Given that services provided by dating portals to minors, and the data processing operations they infer, do not fall under the category of small everyday acts that are usual and necessary to fulfil a child's basic needs, the NAIH believes that adequate consent can only be constituted along with the legal guardian's consent, and not only the child's one.

One must strive to enforce the above stated rules even if it is truly difficult to verify parents' consent. Otherwise, the website's owner or operator facilitates the availability of children for romantic or sexual relationships, which can contribute to their victimization.

We cannot close our eyes on the fact that children can appear on dating websites and be available on websites created to promote the establishment of new relationships. We cannot ignore, and thereby passively approve, such practices. This needs to be asserted even despite the knowledge that registration rules and processes can easily be circumvented. In that case indeed, the problem lies not in the data controller's behaviour, but in the field of child-parent relations, and becomes part of a larger social problem.

EU institutions also underline the importance of this theme (see the Article 29 Working Party's opinion 5/2009 on social networks, Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006, as well as the Commission's COM (2011) 556 report on children's protection in a digital world). It should be noted that Member States provide varying levels of protection. Only a small fraction of contents that are harmful for the healthy growth of children originate from Hungary. A far greater portion comes from other Member States and from outside of the EU. This renders the realisation of a unified protection strategy difficult. Until then, however, the NAIH wishes to enforce and achieve the maximal level of protection possible

regarding data processing operations aimed at children, and also regarding the filtering of contents available to them.

This is why the NAIH investigated the registration processes of no less than 50 dating websites. The NAIH tried to establish whether it was possible or not for minors to register without their parents' consent. Over the course of our test registrations, the NAIH was led to launch administrative data protection procedures against 18 websites. In total, about 4200 profiles[2] were found of minors below 16. The youngest user was only 10 years old. All of those profiles were available online, with the aim to help the establishment of relationships. As a result, the NAIH imposed fines amounting to 2 900 000 HUF[3] in total (close to 10 k Euros), and forced data controllers to erase relevant data and change their data protection policies.

Over the course of the procedures, data controllers were globally cooperative, and deleted the illegally processed personal data, that is to say, the profiles of minors below 16. They modified their procedures and raised the registration age limit accordingly to our demands.

b) The construction of a common marketing database

The NAIH investigated in the frame of an administrative data protection procedure the data processing operations of two companies operating marketing databases. The source of the collected data was registration of the companies' websites. The two companies transferred shared the collected data between one another, and sent emails and SMS messages to the registered users. Telemarketing activities were conducted at a sub-contractor's call centre. Their aim was to advertise various banking and insurance products. Their partner would call people using the company's identity, to promote their own offers or that of others to people registered in either of the two companies' databases. Personal data was therefore received and used by the call centre, and not by the original data controllers collecting the data.

The NAIH established that the investigated operations did not comply with the adequate information requirements, and that the operation's indicated purpose ("marketing purpose") was too vague. There was a total lack of legal basis, for instance the data subjects' consent, for the transfer of personal data by both companies to a partner that was not even named in the general terms and conditions. Both data controllers also failed to provide adequate and precise information and ask for deliberate opt-in. Furthermore, the notification sent to the NAIH for prior registration purposes failed to mention all the involved agents.

Given the established infringements, the NAIH decided to impose a fine, request the adaptation of privacy policies and data protection practices to the Privacy Act's requirements, and require the deletion of illegally collected data.

c) Data breach following a hacker attack

A company collected personal data in the frame of a lottery game for direct marketing purposes, with the data subjects' consent. The company on it’s website also gave access to a 3D game for the registered users. After the marketing campaign was over, the data controller left an active link pointing to the database on it’s website. A group of hackers intruded on the database server. They uploaded the stolen data on several websites, including names, e-mail addresses, phone

2 If data from 2012 is also included, this figure is raised to 7700 profiles

3 If data from 2012 is also included, this figure is raised to 5 900 000 HUF

numbers, dates of birth, city names and in some cases, the password. This data breach concerned more than 50 000 people.

Given the economic size of the data controller, the NAIH considered it to be its responsibility to implement the most efficient data security measures. This charge was aggravated by the fact that internal audits already brought attention to the fact that especially in the face of remote access, these data were not adequately protected.

d) Biometric systems

Among the cases on biometric systems, some were consultation requests by organisations contemplating the introduction of biometric locks or entrance systems. Following its usual standpoint, the NAIH stressed that, given the provisions of art. 4 of the Privacy Act, it is necessary for the use of biometric systems to be adequate, relevant and proportionate. This infers the requirements for the necessity of the use of such data, its proportionality, and the strict evaluation of whether or not it would be possible to achieve the same goal by other, less intrusive means. Furthermore, the NAIH continued to base itself on the conclusions contained in Opinion 03/2012 of the Article 29 Working Party on the development of biometric technologies, and especially those related to how the proportionality of such processing operations should be evaluated. According to such principles, a continuing concern are projects by schools to introduce biometric entrance systems. Indeed, such systems are not indispensable to either the safety of interested parties or that of school property. Finally, the desired purpose of such a system can be attained by less invasive means from the point of view of civil rights.

The NAIH also examined cases where undertakings wished to implement a fairly common device, a fingerprint reader, on cash registers, to limit their access to authorized personnel. The NAIH reminded such companies that according to the art. 10 paragraph 1 of the Labour Code, “only declarations or data relevant to the establishment of labour relations, the carrying out of this relation, or its termination, can be requested from an employee, and only as long as such requests do not violate his civil rights”.

According to the Labour Code, there are two conjunctive conditions that the employer must fulfil so that he can process his employee's personal data. Among the two, the fact that such a processing must not violate his civil rights is the most important one. If this condition is unfulfilled, then the other criterion becomes irrelevant. In examining whether or not civil rights are respected, one must take into account art. 9 paragraph 1 of the Labour Code, which provides that subjects of this law must have their civil rights respected. The rights of an employee may only be restricted if it is directly and without doubt necessary in the frame of the labour relations. Employees must be informed prior to the implementation of such restrictive measures.

Article 9 of the Labour Code provides for the general rules and main principles on the scope of employees' civil rights in labour relations, and on their potential restrictions. In order to protect such civil rights, the Law provides for two strict procedural obligations employers must respect. This procedure must be exclusively and directly tied to the employer's proper functioning. It may not exceed these boundaries. Even the notion of proper functioning is to be strictly interpreted. The employer may only decide to undertake such a procedure if it is obviously and objectively necessary. From this point of view, it is indeed relevant to take into account the employer's interest in making sure only authorized personnel is able to access cash registers and the money it contains. Controlling access to cash registers therefore fulfils the objective criterion of legitimate interest. But beyond this criterion, the Labour Code also enforces the criterion of proportionality. The Article 29 Working Party has defined guidelines in this regard.

Based on the above, the NAIH established that the implementation of fingerprint readers on cash registers was not proportionate, as the purpose it fulfils can be attained through less invasive means in terms of civil rights, like cash registers with increased safety that could only be opened by the use of a special code, given by the employer to its authorized employees.

One of last year's novelties was the introduction in Hungary of voice recognition as a biometric system. This technology is being actively developed. The Data Protection Working Party observed that “testimonials published by manufacturers report that, by implementing such technology, financial services companies have increased fraud detection rates and enabled a faster service to settle genuine claims.” This practice hasn't really taken roots in Hungary yet. Most service providers and producers are still working on introducing their products and services on the local market. In any case, the NAIH is keeping an attentive eye on further developments.

e) “Key to the World of the Net” project

The NAIH launched its first long-term study project, called “Key to the World of the Net”, which focuses on children’s rights in an on-line environment. The conclusions of this 120 page study, conducted by both internal as external experts from our partners, and including also a summary of international best practices, helped us prepare our own educational material for children and educators.

This study is divided into five sections as follows:
(1) basic rights of children, and human rights organizations dealing with the enforcement of children’s rights;
(2) major risks posed by the internet, and the techniques how to recognize them;
(3) best practices from abroad;
(4) institutions in Hungary empowered to protect and support minors in case of abuses;
(5) guidance to safe internet use.

The leaflet is available in Hungarian, English and French on our website.

Complaints
During 2013, the Office of the Data Protection Commissioner opened 910 complaints for investigation.

Complaints from individuals in relation to difficulties gaining access to their personal data held by organisations accounted for almost 57% of the overall complaints investigated during 2013. With 517 complaints in this category, this represented a record high number of complaints concerning access requests.

Complaints in 2013 about unsolicited marketing communications under the Privacy in Electronic Communications Regulations (S.I. No. 336 of 2011) were at a similar level to recent years with a total of 204 opened for investigation. Once again, 2013 saw a number of prosecutions taken against some of the major companies in the telecommunications sector in relation to marketing offences.

In 2013 the Commissioner made a total of 29 formal decisions. 25 of these fully upheld the complaint, 1 partially upheld the complaint and 3 rejected the subject of the complaint.

Data Security Breaches
In 2013, the Office of the Data Protection Commissioner dealt with 1,577 Data Security Breach notifications. These included the first notifications made using the new online reporting mechanism laid down in European Commission Regulation 611/2013 which sets out specific rules for the notification of data security breaches by Telecommunications and Internet Service Providers.

In line with the wish of the Office to work effectively with other Data Protection Authorities, joint investigations into data breach notifications made to the Office by two multi-national companies were instigated in conjunction with the Office of the Privacy Commissioner in Canada. These investigations are ongoing and it is hoped they will be concluded in 2014.

Audits
The Office of the Data Protection Commissioner audited 44 organisations during 2013. This was an increase of 10% on the number of organisations audited in the previous year.

Annual Report of the Data Protection Commissioner
The Annual Report of the Data Protection Commissioner for 2013, which provides further information in relation to the activities of the office of the Data Protection Commissioner during 2013, is available at:
http://www.dataprotection.ie/docimages/documents/Annual%20Report%202013.pdf

ITALY / ITALIE

Major developments in the data protection field

January 2013-May 2014

Italy

Data Protection Code (Legislative Decree no 196 of 30 June 2003)

Section 19, para 3-bis of the Data Protection Code was repealed by section 53(1)(e) of legislative decree no. 33 of 14 March 2013. However, the wording of the paragraph in question was shifted to section 4(5) of the said legislative decree ("*The information concerning performance of the tasks committed to any person that is in charge of public functions including the respective evaluation shall be made available by the public employer. Except where provided for by law, no information may be disclosed concerning nature of the medical conditions and/or personal or family circumstances resulting into a person's absence from the workplace or else the elements making up the evaluation or any information on the employment relationship between the aforementioned public employee and the public employer if they are suitable for disclosing any items of information referred to in section 4(1)d. hereof.")*.

The up-to-date version of the Data Protection Code is available in English at the following link:

http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf

Main activities of the Italian Data Protection Authority

Data processing in the public sector

The DPA gave its opinion (7 February 2013) on the draft legislative decree (adopted on 14 March 2013 – No. 14) which sets forth specific transparency obligations public bodies have to comply with (e.g. through publication on their institutional web sites). The Garante signaled some criticalities of the draft text and provided specific suggestions aiming at reconciling transparency and the protection of personal data, such as: avoiding the dissemination of particular categories of data, namely those related to individuals' health; preventing the data published on line from being retrievable by means of general search engines such as Google (but only via internal search engines); setting out of the period during which posting of data on websites can be regarded as proportionate in view of achieving transparency purposes; limiting the publication of data related to public sector employees only to those data which are strictly relevant; in respect of holders of political offices, limiting the obligation to publish data both with regard to the range of individuals involved and to the content of the information to be published.

Countering tax evasion

The DPA, following specific investigations, prescribed measures to be adopted in respect of the processing carried out by the Revenue Agency aiming at the concise assessment

of individuals' income to counter tax evasion (21 November 2013). The measures were meant to ensure that the anti-fraud activity in question was carried out with due respect for the protection of personal data; they consisted, in particular, in specific adjustments to be made by the Agency regarding the criteria for taxpayers' profiling and for the selection of the individuals subject to investigations; further, arrangements were laid down in respect of data quality; data retention; information to be provided to data subjects regarding the processing of data and the possibility to be heard by the Agency.

Justice

The DPA set out measures and arrangements public prosecutor's offices in Italy will have to implement in order to enhance the security of any personal data they collect and use as part of intercepted communications (24 July 2013). The measures include both physical security measures (such as access to premises only via individually allocated badges associated with a numerical code or biometrics-based devices; logging of all accesses; CCTV monitoring of premises) and IT security arrangements (such as use of dedicated workstations and strong authentication procedures for operator access to systems and servers; logging of all interception-related activities; encryption-protected copying to removable media; encrypted storage of original records and back-up copies; use of secure network protocols for data exchanges between judicial authorities and ISPs).

Intelligence services

Following Edward Snowden's revelations, a Memorandum of Understanding was signed by the Italian DPA and the Department of Information Security of the Presidency of the Council of Minister (11 November 2013). The MoU aims at completing safeguards for individuals' rights concerning data processing for intelligence purposes in particular with regard to the investigations carried out by the Garante, namely in respect of the access to databases held by public bodies and the access for cybersecurity purposes.

Health data

The adoption of adequate safeguards was prescribed by the DPA (10 January 2013) in order to ensure that the personal data contained in health files would be managed only by the health practitioners treating the patient and shared with other professionals only with the data subject's consent.

Marketing

The DPA intervened on several occasions in the field of marketing. It issued Guidelines on marketing and against spam (including the so called social spam, viral marketing and targeted marketing) laying down a first consolidated set of measures and precautions that can be helpful both to the companies that plan a marketing campaign to advertise their products or services and to any individual wishing to fend off advertising without consent (4 July 2013). The DPA clarified via a separate decision that it is enough to obtain consent once for all marketing activities – such as sending ads or performing market surveys; the consent provided to receive automated promotional messages (emails, SMS-texting) also applies to such messages when sent via less privacy-intrusive channels such as paper mail or through operator-assisted phone calls, providing users

are informed appropriately and enabled to freely express their respective preferences (15 May 2013). Detailed rules were set forth for public and private bodies planning to rely on call centers located outside the EU. As well as recalling the requirements to be met for transferring personal data (in particular, customer data) to third countries, the DPA ordered the controllers concerned to provide specific information to their customers and afford them the option to select operators located in Italy as regards incoming phone calls (10 October 2013). Specific measures were laid down by the Garante and submitted to public consultation to prevent silent calls, which are a major source of concern for users. The measures include, in particular, termination of silent calls (i.e. when no operator is available to take up the call) within 3 seconds from pick-up by users; setting of a threshold of 3 silent calls every 100 successful calls (per single telemarketing campaign); a ban on re-contacting a user before one week has elapsed from the silent call; storage of statistics on silent calls for at least two years to enable oversight.

Telco databases to check clients creditworthiness

Another public consultation was launched by the Garante (mid-April 2014) on a draft decision setting forth the requirements to be met by telecom operators in order to participate in and manage the future "Integrated Information System, IIS", which they will be allowed to use in order to check creditworthiness before stipulating new contracts. The system will be working on the basis of an agreement entered into by the parties concerned (telecom operators and IIS manager), which will have to be submitted to the Garante beforehand for prior checking purposes. The IIS will be fed and accessed by providers of electronic communications services and will only contain information on payment defaults; no sensitive or judicial data may be processed and no other purposes may be served by the IIS, which will have to be kept logistically and physically separate from other databases managed by the given provider. Whilst the Garante determined that customers' consent would not be necessary to process such data (based on the balancing of the interests at issue), only information on customers defaulting after three months from termination of the respective contracts may be included and only if the debt is in excess of 100 Euro; customers must be informed by the operators before their default is recorded in the database. Specific rules were also laid down regarding the information to be provided to customers on the functioning of IIS; moreover, the mechanisms and timeline were clarified for operators to expeditiously update the information in the IIS following remedial actions taken by customers.

Mobile payments

A public consultation was launched in January 2014 concerning the DPA's decision (12 December 2013) on mobile payments setting forth specific safeguards to protect the personal data of users who, by charging directly their phone bills, make payments at a distance using the so-called mobile remote payment systems.

The safeguards – which include a specific information notice, consent in case of marketing and profiling; security measures, data retention policies - are addressed to the three main stakeholders involved in mobile payment services (the carriers, i.e. electronic communications providers; payment hubs supplying and managing the technological platforms for such services; the merchants offering and selling digital contents, multimedia and other products).

Google Street View

The DPA sanctioned Google by a 1-million-Euro fine because of Google's Street View service in December 2013 by having regard, in particular, to the circumstance that the unlawfully collected information had been pooled into a large database – the one set up by Google in connection with the Street View service; furthermore, the Garante decided to rely on the provision in the Privacy Code that is aimed at ensuring effective sanctions are imposed on major business entities - given that Google's consolidated turnover for 2012 totaled over 50 billion dollars.

Traffic data

During 2013 the DPA continued its inspections on the storage of traffic data and sanctioned those communication providers who were found not to be compliant with the measures imposed for this sector since 2008.

Data breaches

The DPA adopted a general decision replacing previously adopted Guidelines, in pursuance of paragraph (6) of section 32-bis of the Code (implementing Directive 136/2009/EC) in order to provide guidance and instructions on the circumstances under which electronic communications service providers are required to notify personal data breaches, the format applying to such notification, and the relevant implementing arrangements (4 April 2013).

Graphometric authentication techniques

The DPA granted two prior-checking applications from banks intending to use graphometric authentication techniques for customer identification. The DPA requested that the purpose limitation principle should be complied with strictly and that fallback procedures be available for those users who do not wish or are not able to rely on this authentication method; data retention arrangements will also have to be compliant with the proportionality principle.

Biometric data

Via a decision of mid May 2014 submitted to public consultation the DPA outlined the cases where it will be no longer necessary to apply for prior checking with a view to the adoption of biometric systems provided that specific measures for the protection of personal data are fully respected.

According to this decision the use of fingerprints for physical access to restricted areas, or for the activation of electronic devices is allowed without any need for prior checking by the DPA. Fingerprints and hand geometry can also be used to simplify the physical access of users to physical areas, whether public or private (e.g. libraries, or restricted airport areas), or to services (e.g. safe deposit boxes), but only with the data subject's consent and provided alternative arrangements for those who do not want to use biometric devices are made available. No prior checking is needed for the use of graphometric signature to undersign electronic documents. The creation of centralized biometric archives, and the use of biometric data for purposes other than those specified are not allowed.

23 May 2014

Country report
Principality of Liechtenstein

Legal developments:

The ordinance on the accreditation of data protection certification procedures and on the introduction of a data protection quality label entered into force in February 2014. In order to increase the protection and safety of data, the manufacturers of systems or programmes for data processing as well as private individuals or authorities processing personal data may have their products, systems, procedures, and organisation assessed by recognised independent certification bodies.

In 2014 the new legal framework for a new settlement system in the health sector entered into force. The reimbursement for inpatient treatment is administered through the DRG-System (Diagnosis Related Groups System). Insurances are required to establish a certified data collection point that generally receives the invoices in the DRG-System. The Data Protection Office publishes a list of the certified data collection points.

Other developments:

Big Data entails a challenge to key privacy principles. Guidelines to highlight the privacy challenges associated with Big Data were published. It is hoped that these guidelines will be helpful in practice, in particular, considering new developments in the field of “big data”.

A steadily raising number of enquiries regarding the processing of personal data in the working area led the Data Protection Office to release respective guidelines. These guidelines provide general information on how personal data may be processed at the working place illustrated by numerous practical examples and case studies. Starting with the recruiting process to the point to the certificate of employments and retirement, the major procedures of the different stages in a working life are highlighted. These guidelines shall clarify the legal requirements of processing personal data for employers as well as for the employees or employment services in order to enhance legal certainty.

Awareness-raising activities

At the occasion of the European Data Protection Day, a public event was organized together with the University of Liechtenstein on the subject *“How healthy is big data? Opportunities and risks of collections of personal data in the healthcare system”.*

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

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

1. Recent National Developments – legal framework

1.1. No changes of the *Law on Legal Protection of Personal Data of the Republic of Lithuania* since year 1211, when the last amendments and supplements have been made.

1.2. The Law on Electronic Signature was amended on 17th December 2013 in connection to an instruction of the State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – the SDPI).
A person had lodged a complaint because the state enterprise had used personal identification number in the certificate of an e-Signature without a legal bases. There had not been a provision requiring to use personal identification number in the certificate of an e-Signature in Lithuanian legal acts till 17th December 2013. The SDPI gave a legally binding instruction to the state enterprise not to use personal identification numbers in the certificate of an e-Signature in 2011. The Supreme Administrative Court sustained the position of the SDPI and prohibited to use personal identification number in the certificate of an e-Signature.
The amendment of the Law on Electronic Signature of 17th December 2013 that entered into force since 1st January 2014 legalised the use of personal identification numbers in the certificate of an e-Signature.

2. Major case law

2.1***. Processing of personal identification number***

A person lodged a complaint because a company providing internet and cable television services asked the complainant to sign a standard contract and to write his personal identification number in the contract. According to paragraph 2 of the Article 7 of the Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter – the LLPPD) it shall be permitted to use a personal identification number when processing personal data only with the consent of the data subject. Paragraph 3 of this Article determines exceptions to this rule. The SDPI stated that the consent of the complainant was not free because otherwise he would not get the service and gave a legally binding instruction to the company to change the form of the standard contract and not to require personal identification numbers of their customers. This instruction was appealed to the Vilnius District Administrative Court by the complainant. The Court dismissed the appeal as unfounded, concluding that the decision of the SDPI that the consent of the complainant had not been freely given was correct. The complainant appealed this decision to the Supreme Administrative Court, which also stated that the instruction of the SDPI had been correct and the arguments of the company that the personal identification number is necessary in the contract are not important in this case.

2.2. *Application of the Law on Electronic Communications for legal persons*

An Irish Company lodged a complaint that they had received calls from representatives of a Lithuanian company, trying to sell them a product.
According to paragraph 1 of Article 69 of the Law on Electronic Communications of the Republic of Lithuania (hereinafter – the LEC) the use of electronic communications services, including

electronic mail, for the purposes of direct marketing may only be allowed in respect of subscribers or registered user of electronic communications who have given their prior consent.
The SDPI decided that the fact that telephone numbers of the Irish company were published on the internet does not give the right to use these telephone numbers for the purposes of direct marketing and gave an instruction to the Lithuanian company to ensure that electronic communications services for direct marketing purposes were used only with the prior consent of the subscriber, including publicly published telephone numbers.
This instruction was appealed to the Vilnius District Administrative Court. The court decided that the SDPI as the institution responsible for personal data protections is authorized to investigate only complaints of natural persons, but not complaints of legal persons as it was done in this case.
The SDPI appealed this decision to the Supreme Administrative Court, which stated that the authority of the SDPI is not differentiated, according to which subjects (natural persons or legal persons) the provisions of the LEC are applied. There is not a reason to state that the definition of subscribers covers only natural persons. The Supreme Administrative Court decided that decision of the court of the first instance was not correct and the SDPI is authorized to investigate complaints of legal persons according to the LEC.

2.3. *The right of an advocate to collect data from the database of the Real Estate Registry*

A person lodged a complaint because he received a call from the advocate, to whom his personal data (name, surname, date of birth, data about real estate he owns) was given. Advocare informed the SDPI that data have been collected data from the Real Estate Registry on a basis of undertakings according to the contract. Personal data were collected in order to reach the owner of that property. SDPI made a decision these data were collected with no legal background for data processing.

The decision was appealed to the Vilnius Discrict Administrative Court stating that SDPI's decision was unlawful, because the data collected for the purpose of the contract and from open public register.

The Court dismissed the complaint and decided Court decision was that any of indicated that in this case processing of personal data should be implemented according to the law and did not comply requirements of the contract of representation.

3. Preventive activity

3.1. *Consultations*

Seeking better understanding requirements of data protection laws the SDPI provides consultations by telephone, by e-mail, by mail and organizing meetings of data controllers. 6 public consultations have been published in year 2013, also delivered 1075 consultations to data subjects and 2770 – to data controllers.

3.2. *Inspections on the SDPI initiative*

SDPI made 51 planned investigations on its' initiative in year 2013 in total. Inspections were conducted in companies providing e-shopping services in order to determine whether the aforementioned companies, processing data of the customers ensures proper implementation of data subject's rights, legitimacy of data retention and right of access. Any violations of the laws on data protection were not found only in 3 companies.

3.3. *Coordinated inspections executed by of Estonian, Latvian and Lithuanian SDPA*

In year 2013 Estonian, Latvian and Lithuanian data protection supervisory authorities (hereinafter – Baltic SDPI) conducted coordinated inspections in frame of Baltic States cooperation. Baltic SDPI checked the lawfulness of clients' and employees' data processing and

video surveillance in 4 gambling Companies by general questionnaire of data protection supervisory authorities of three Baltic States.
All the 4 gambling Companies violated Republic Of Lithuania Law On Legal Protection Of Personal Data. During investigations several incompatibilities to personal data protection requirements were established and orders to the Companies given.

4. Public awareness

4.1. Data Protection Day in year 2014
In aim to raise data protection awareness European Data Protection Day was celebrated on 28th January 2013. Annual press conference "Personal data protection in European Union and Lithuania" in Seimas (Lithuanian Parliament) took place on January 28th. Main topics at the conference were personal privacy vs modern technologies and how to make consultations on personal data protection issues more convenient to the citizens.
As well conference "Personal Data Protection 2014: Innovations, Topics, Case Studies" was organized on January 30th. One of the main topics at the conference was on personal data protection issues related to personal identification in e-space issues and cyber security, how to ensure proper processing of personal data in case of breaches in cyberspace. These topics are of high importance for the all society because in case of data breaches the damage is resulting from the unauthorized identification in e-space or even unlawful activity in cyberspace.

4.2. *Cooperation agreement with Mykolas Romeris University*
24th February 2014 cooperation agreement was signed between SDPI and Mykolas Romeris University, faculty of Social Technologies. Two parties became social partners and plans are made to cooperate in implementing a study programme "Managing of cyber security" as well as constant exchange of information on related topics.

4.3. Project with Lithuanian Librarians Association
29th April 2014 conference organized by SDPI together with Lithuanian Librarians Association (hereinafter – LLA) took place. Project "Augmenting the cooperation between State Data Protection Inspectorate and Lithuanian Librarians Association, by implementing politics of personal data protection" started June 4th 2013 and will end in December 2014. The aim of the project is to ensure better implementation of personal data protection principles. During the project about 200 librarians from all over the country attended seminars on personal data protection related topics and are now able to help citizens to deal with related issues, help them to fill the forms or provide basic consultations.

4.4. *Traffic recorders*
The use of traffic recorders has increased recently in Lithuania and processing of personal data by using these devices is complicated. In order to discuss issues, related to the use of traffic recorders the meeting with the representatives of Ministry of the Interior, the Police Department and the Ministry of Transport was held at the Inspectorate on February 10th 2014.

MONACO

Les développements majeurs survenus dans le domaine de la protection des données à Monaco depuis la dernière session plénière :

1.

- Loi n° 1.402 du 5 décembre 2013 portant approbation de ratification de la Convention sur la cybercriminalité du Conseil de l'Europe,

- Loi n° 1.401 du 5 décembre 2013 relative à la prescription civile,

- Loi n°1.399 du 25 juin 2013 portant réforme du Code de procédure pénale en matière de garde à vue. Ce texte régit les enregistrements vidéo pris en garde à vue et leur durée de conservation,
- Ordonnance n°4.221 du 19 mars 2013 Réglementation des missions et de l'activité de l'Institut Monégasque de la Statistique et des Etudes Economiques,
- Ordonnance Souveraine n°4.694 du 30.01.2014 fixant les conditions d'application de la loi n°1165 du 23.12.1993, modifiée, qui a précisé les modalités d'application de la loi sur la protection des informations nominatives en ce qui concerne les traitements ayant pour finalité la recherche dans le domaine de la santé,
- Arrêté Ministériel n° 2013-156 du 19 mars 2013 modifiant l' Arrêté Ministériel n° 66-055 du 9 mars 1966 portant attribution d'un numéro d'identification aux établissements industriels, artisanaux, commerciaux et autres et rendant obligatoire l'utilisation de ce numéro d'identification pour les classifications et les statistiques officielles,
- Arrêté Ministériel n° 2013-234 du 22 avril 2013 créant le Répertoire du Numéro d'Identification Statistique (N.I.S.),
- Arrêté Ministériel n° 2013-235 du 22 avril 2013 modifiant l'Arrêté Ministériel n° 2006-220 du 28 avril 2006 relatif à la détermination d'un Produit Intérieur Brut (PIB) et un Revenu National Brut (RNB),
- Arrêté Ministériel n° 2013-155 du 19 mars 2013 fixant une mesure d'ordre statistique en application de la loi n° 419 du 7 juin 1945 relative aux mesures d'ordre statistique,
- Arrêté Ministériel n° 2013-270 du 27 mai 2013 modifiant l'Arrêté Ministériel n° 2000-440 du 18 septembre 2000 relatif à la commission chargée de procéder aux opérations de recensement,
- Décision du Tribunal Suprême du 25 octobre 2013 déclarant l'article 18 de la loi n°1165 relative à la protection des informations législatives sur la procédure d'investigation de l'autorité de contrôle non conforme à la Constitution. La Haute Juridiction a estimé que ledit article 18 portait une atteinte au principe de l'inviolabilité du domicile consacré par l'article 21 de la Constitution, non proportionnée au but d'intérêt général poursuivi par loi, en l'absence de garanties effectives et appropriées tenant compte de l'ampleur et de la finalité des pouvoirs de l'autorité de contrôle.
Eu égard à cette décision, l'Etat monégasque a engagé une réflexion de fond en la matière, et plus précisément, sur les pouvoirs d'investigation de l'Administration.

2.

La CCIN a émis les recommandations suivantes :
- 27.11.2013 : recommandation n° 2013-129 sur les déclarations de traitements automatisés d'informations nominatives concernant « l'organisation des élections des délégués du personnel instituées par la loi n° 459 du 19 juillet 1947, modifiée »,

- 27.11.2013 : portant recommandation n° 2013-128 sur les déclarations de traitements automatisés d'informations nominatives concernant « La gestion administrative des salariés »,
- 21.10.2013 : recommandation n° 2013-121 sur l'instauration de règles internes relatives à la procédure d'alerte en cas de violation de données à caractère personnel par les organismes monégasques - prestataires de service ou sous-traitant - de fournisseurs de services de communications électroniques soumis à la législation européenne.
- 16.09.2013 : recommandation n°2013-147 sur les traitements automatisés d'informations nominatives ayant pour finalité « la gestion des obligations issues de la réglementation dite « FACTA ».

Isabelle ROUANET-PASSERON
Conseiller Technique
Département de l'Equipement,
de l'Environnement et de l'Urbanisme

I. Legislation

1. Data protection law

In the reporting period since the last TP-D plenary meeting in October 2013 there were no changes in the Polish law on personal data protection. In the committees of the Lower Chamber of the Polish Parliament (Sejm), works are still being conducted on the change introduced in "deregulation law". According to the proposal data controllers will be exempted from the obligation of data filing systems' registration, if they do not process sensitive data and appoint and notify a Data Protection Officer to GIODO.

2. e-Government

2.1 Amendment of the Act on computerisation of entities performing public tasks

On 11th May 2014 changes, introduced in the Act of 10th January 2014 on the amendment of the Act on computerisation of entities performing public tasks as well as some other acts, came into force.

Amendment of the aforementioned Act brings in alternations to conditions of deliverance of letters to citizens by electronic means. At the time being, an office can send letters to citizens under the condition that citizen has requested such means of delivery or expressed his/her consent. After the amendment, sending of letters by offices with the use of electronic means will be obligatory, if in a given case citizen sent a letter by such means or requested such form of communication.

There have been also changes in the rules of delivery. Currently, in case of sending an answer by electronic means and lack of acknowledgment of receipt, an office is obliged to send after 7 days from sending of letter by electronic means another one by post. After the change of provisions, an office, if there is lack of acknowledgment of receipt, shall be obliged to send this letter again by electronic means. In case of lack of acknowledgment of receipt in 14 days from the date first letter was send it is deemed to be delivered.

Electronic system used for delivery of letters to citizens by electronic means has to ensure confidentiality of data transmission as well as authorisation with qualified certificates or ePUAP trusted profile.

2.2. Computerisation of the judicary

The Inspector General for Personal Data Protection expressed its reservations to the legal act proposals, according to which the Minister of Justice would be a data controller for personal data processed by independent courts. GIODO pointed out sensitive nature of data that are being processed by the courts as well as the rule of separation of powers, which in its opinion is infringed by the aforementioned proposal. It also highlighted that Ministry of Justice should support the courts in computerisation, but not on the terms enabling direct intrusion in documents being processed.

II. Inspection activity

Inspection at a company, to which the Ministry of Justice commissioned delivery of letters issued by the courts.

In the first quarter of 2014 GIODO commenced inspection in the points of collection of letters issued by the courts. An entity that won tender for delivery of letters issued by the courts, due to its lack of developed network of points of delivery, was signing agreements, commissioning this task to other entities such as florist's, chemist's, groceries etc., where letters were left if the courier found no one in. Complaints were filed by citizens concerning inappropriate safeguards of the letters left at those entities, as well as difficulties with finding them, for advice note did not indicate that the collection point was a florist's or chemist's. The results of first inspections are being prepared.

Inspections in connection with the Varsovian Card.

GIODO conducted inspections at the Public Transport Authority in Warsaw (ZTM), the Office of the Capital City of Warsaw and the Ministry of Finance, in connection with exchange of data on citizens (taxpayers) between those institutions for the purposes of issuing the Varsovian Card, which allows people who live in Warsaw and during the taxable year filed a tax return for the previous year in revenue office in Warsaw to use cheaper long-term tickets. GIODO's inspection confirmed that the above mentioned exchange of data was illegal due to violation of the provisions on personal data protection.

GIODO's inspections showed that the Office of the Capital City of Warsaw, although it did not have a legal basis, was collecting information on the place of PIT (personal income tax) settlement, and the Finance Ministry provided that information to the above Office, although it also did not have legal grounds for it, as neither the resolution of the City Council nor the Data Processing Agreement between the above Office and the Ministry of Finance could be regarded as such ground.

In connection with the found irregularities GIODO will institute administrative proceedings against the three institutions, which will be aimed at restoring the proper legal state.

Moreover, GIODO is considering possible informing relevant authorities, e.g. Ombudsman, about its doubts, as to whether such a card addressed only to the citizens of a given city can even exist and whether it does not lead to limiting a free flow of persons incosistent with the Euroepan law.

III. Events

8th Data Protection Day - 28 January 2014

On the occasion of the European Data Protection Day, which was celebrated in Poland for the eighth time, on 28 January 2014 the Inspector General traditionally organised an Open Day for all citizens. During the Open Day everyone had an opportunity to obtain legal advice as well as educational and informational materials. On the same day a conference under the slogan "Privacy in Digital World" was held. It comprised both lectures and discussion with participants. Also, as usual the European Data Protection Day was celebrated in Brussels, where Dr Wojciech Rafał Wiewiórowski held a meeting with Members of the European Parliament (21

Jan.), attended a Conference on the occasion of the 10th anniversary of the European Data Protection Supervisor and he took active part in the 7th International Conference on Computers, Privacy and Data Protection (22-24 Jan.), specifically in the panel on the European data protection reform. Also in Brussels GIODO organised, for the eighth time, the celebration of the 8th Data Protection Day (21 Jan.), in cooperation with and at the premises of the Permanent Representation of the Republic of Poland to the EU. The event was attended by Data Protection Commissioners of the EU Member States, headed by Mr. Peter Hustinx- European Data Protection Supervisor, representatives of the Polish ministries and central offices, visitors from the European Commission, Council of Europe, Members of the European Parliament and representatives of diplomatic missions in Brussels.

Also, on 28 Jan. 2014 events were organised at schools which participate in the programme realised by GIODO – "Your data – your concern. Effective protection of personal data. Educational activity addressed to students and teachers". The programme is an undertaking aimed at developing effective methods of educating children and youth on personal data protection and the right to privacy.

VI. GIODO projects and programmes

GIODO has just finalised realisation of the mobility project financed from the resources of the European Union within the framework of the Leonardo da Vinci Project, being part of the "Lifelong Learning Programm". The project enabled the employees of the GIODO Bureau to exchange the knowledge and experiences in law enforcement in the field of data protection with authorities from partner countries dealing with similar issues, where they completed internships.

Since 2012 GIODO has been realising another project financed from the resources of the European Union within the framework of the Leonardo da Vinci Project, being part of the "Lifelong Learning Programme" entitled „Raising awareness of the data protection issues among the employees working in the EU", in cooperation with the Czech, Bulgarian and Croatian DPA. The project is aimed at developing educational materials for the natural persons undertaking employment or working in one of the countries participating in the project. The project is to be finalised by the middle of 2014.

In 2013 the PHAEDRA project (Improving practical and helpful cooperation between data protection authorities) co-funded by the European Commission under the programme Fundamental Rights and Citizenship "Action grants" was launched. GIODO participates in the project as member of the project consortium. The project is realised in cooperation with Vrije Universiteit Brussel (project coordinator), UK Trilateral Research & Consulting LLP (partner) and Spanish Universitat Jaume I (partner). The basic objective of the project is to identify the problems hampering cooperation between particular data protection authorities and other state entities dealing with this issue as well as to draw up recommendations aimed at improving the situation. As a result the project will contribute to improving co-operation and co-ordination between all stakeholders. The project is to be finalised in 2015.

Poland wide programme "Your data, your concern. Educational initiative addressed to students and teachers" is an undertaking being realised by the Inspector General for Personal Data Protection (GIODO) under honorary patronage of the Ministry of National Education and the Ombudsman for Children since 2009.

The main objective of the programme is to include the issues related to personal data protection and the right to privacy in the curricula of teachers vocational training centres, primary and middle schools in Poland. One of its stages consists in training school teachers and providing them with education materials including among others information on personal data protection principles, lesson scenarios, multimedia presentations and teaching aids helpful in realising the programme, as well as in preparing teachers to shaping informed responsible attitudes among pupils. The next element of the programme is conducting courses related to personal data protection in schools as well as active participation of students and teachers in events organised within the framework of the European Data Protection Day.

The programme „Your data –your concern" is addressed to teachers, guidance counselors and students at primary and middle schools all around Poland. It is possible to join the programme for primary and middle schools and teachers vocational training centres, and the pilot programme – for secondary schools.

209 education establishments, including primary, middle and secondary schools, and teachers vocational training centres, from all voivodeships, participate in the 4th edition of the programme for the academic year 2013/2014.

Within the framework of the programme, GIODO organises a competition for students of primary, middle and secondary schools aimed at creative presentation of reflections on personal data protection as well as a competition for education establishments participating in the programme. As regards the latter competition, GIODO presents a "Golden Feather" statuette to selected education establishment for its work for the benefit of dissemination of the right to privacy and data protection among students and teachers.

VIII. Agreements on cooperation

On 25 February 2014 GIODO concluded the Agreement with the University of Social Sciences (Społeczna Akademia Nauk) with the seat in Łódź. It is a subsequent, already 13th university with which GIODO cooperates. The agreement relates to research, educational, promotional and publishing cooperation on the protection of privacy and personal data, classified information and other secrecies protected by law. It provides inter alia for joint organisation of seminars, conferences, training courses and internships as well as performance of scientific and research works among others from the field of personal data protection in the state security systems. The employees of GIODO and the University of Social Sciences are expected to participate in the training courses organised in these institutions.

PORTUGAL

During the period going from the last plenary to the present day (the 25th of May 2014) no new legislation concerning specifically personal data protection was published.

Some legislation was however published regarding very different matters in which the protection of personal data was referred, as in the case of the law concerning clinical investigations.

In general the legislator did not included any specific personal data protection provision preferring instead to refer the direct application of the general data protection law.

Regarding Law 21/2014 of 16th April, “Law on Clinical Investigation”, together with a reference to the application of the general law, the legislator especially emphasized the primacy of the “person” and of fundamental rights over scientific and societal interests, and the essential role of the consent of persons voluntarily involved in medical scientific investigation.

João Pedro CABRAL
Técnico Superior / Legal Adviser
Gabinete de Relações Internacionais/International Affairs Department
Ministério da Justiça/ Ministry of Justice
Direção-Geral da Política da Justiça/Directorate General for Justice Policy

ROMANIA / ROUMANIE

Romania – National Supervisory Authority for Personal Data Processing - Recent developments in data protection field - 31st T – PD plenary meeting:

- **Inter-institutional collaboration with a view of combating SPAM**. The National Supervisory Authority for Personal Data Processing (NSAPDP) organised on the 5th December 2013 a reunion with representatives of the Ministry for Informational Society (MSI) and the National Association of Internet Services Providers in order to establish a series of concrete mechanisms of inter-institutional collaboration with a view of ensuring an effective legal protection of users of electronic communications' services as regards the proliferation of the use of spam messages. The three parties welcomed the proposal to enforce a sanction of blocking internet access, in collaboration with internet services providers via their national association, in cases of repeated transmissions of unsolicited commercial communications to a large number of e-mail addresses, respectively for the illegal trade of data bases containing such personal information, all based on a Decision of the MSI in accordance with Law no. 365/2002, as well as coercive actions undertaken by the NSAPDP on the basis of Law no. 506/2004 (protection of privacy within electronic communications sector) and Law no. 677/2001 (general DP act).

- **NSAPDP Decision on approving the transfer of data to third countries on the basis of Binding Corporate Rules (BCR)**. On the 18th March 2014 the NSAPDP issued **Decision no. 41** on approving a model authorisation for the transfer of personal data based on binding contractual clauses. This Decision comes in support of data controllers who wish to use BCRs as a guarantee in order to transfer personal data to a third country. BCRs are, therefore, considered as sufficient guarantees both as regards the protection of individuals' fundamental rights and liberties, as well as the effective exercise of such rights; these guarantees result especially from contractual clauses subject to authorisation form the supervisory authority prior to the data transfer taking place.

- **Decision of the EU Court of Justice on the data retention Directive**. The provisions of Directive 2006/24/EC were initially transposed into the Romanian legal framework through Law no. 298/2008 which received a negative Opinion from the National Supervisory Authority for Personal Data Processing. This law was later declared unconstitutional by our Constitutional Court in its Decision no. 1258/2009 as it infringed upon the right to intimate, family and private life, the right to secrecy of correspondence as well as right to freedom of expression, in a manner which was inconsistent with the provisions of article 53 of Romania's Constitution (on the conditions under which restrictions may be brought to the exercise of certain rights and liberties). Thereafter, following an infringement procedure started by the European Commission, in order to implement the provisions of Directive 2006/24/EC, Law no. 82/2012 was adopted and it also received a negative Opinion from the NSAPDP for similar reasons, related to the need to observe the individuals' private life. Following the ECJ's Decision, in April this year, inter-institutional consultation procedures were started at national level in order to repeal the law through which the provisions of the data retention Directive were implemented at national level.

- In order to increase awareness amongst the general public with regard to the activities carried out by the **NSAPDP**, from the beginning of February 2014 the supervisory authority has created a **Twitter account**: *https://twitter.com/anspdcp (@anspdcp)*. The supervisory authority's Twitter account is only meant to be used as a quick way to communicate news related to our office, especially those referring to sanctions imposed or various events organised in order to raise awareness on the rules of processing personal data.

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

Country Report – Directorate for Personal Data Protection

Republic of Macedonia

(September 2013 – April 2014)

Institutional developments

PROJECTS

1. The Directorate for Personal Data Protection on 03.02.2014 organized an event to officially launch the project "TECHNICAL ASSISTANCE FOR STRENGTHENING THE ORGANIZATIONAL AND INSTITUTIONAL CAPACITIES FOR PROTECTION OF PERSONAL DATA". The project is focused on protecting the privacy of social media and personal data protection when using Cloud computing applications, and it is implemented and supported by the Ministry of Foreign Affairs of the Kingdom of Norway. With this support it will raise the public awareness about the use of the Internet and it will improve the knowledge about the modern technological development, with emphasis on the transfer of personal data through the use of Cloud computing applications. With the purpose of keeping up with the trends in Europe, it is important to monitor the strategic positions of the European Commission (EU Strategy on Personal Data Protection) in this sphere, with respect to: 1) standards simplification and certification of cloud computing, 2) development of new models, agreements and clauses, and 3) initiating European Cloud Partnership.

What is important to point out from Macedonian perspective is that in practice there are certain conditions or occurrences that have not yet been perceived as "Cloud computing", but for which, *de facto,* the issue of personal data abuse is extremely important. A rising trend among the online services in the business sector, e-stores, although a practice for doing business on internet is around for some time already. In accordance to data of the International Cards System during the year 2011 some 77.000 transactions in electronic trade were conducted, whereas in the year 2013 this figure is expected to reach the number of 265.000 transactions. Since 2007, 300 companies in Macedonia selling goods online have been registered. It is extremely important to achieve successful online transactions at real time, in cases when sometimes a few users need the services of one provider, when there is a need of rapid data

check-up in order to realize the transaction; these are all cases when engagement of massive IT potentials is a must. For all these situations the solution lies in “Cloud computing”. These are all reasons worth enough to draw our attention to this trend.

More on – http://dzlp.mk/sites/default/files/u4/Doc.1a_en.pdf

2. „WITH TRUST TOWARDS BETTER SERVICE” In the period 08.01 – 15.03.2014 the Directorate for Personal Data Protection, EVN Macedonia, BEG Balkan Energy Macedonia and Vodovod Skopje and MRTV, launched the project “With trust towards better service” – update your personal data. During this project, citizens, consumers of the utilities provided by those companies, had the opportunity to update their data through special forms which were sent to them with the monthly bills. A total number of 6 564 citizens from Skopje have exercised the right to update their data and have informed the companies on the changes of their data. All the data that have been selected will be exchanged among the companies upon previously signed Agreement and Procedure.

3. CELEBRATION OF THE EUROPEAN DAY OF DATA PROTECTION , JANUARY 28, by holding a National conference to present the results of the implemented project "Sustainable system for continuous primary and secondary education in the principles of protection of personal data", funded by the European Union. Under the motto "Privacy is mine, although I am a child", the Directorate for Personal Data Protection conducted a competition (literature and art) aimed at primary school students to raise awareness about the misuse of personal data and to increase awareness for their protection. To increase awareness and assist promoted methodical reading for teachers, it was developed within the EU project a separate "Handbook for teachers to learn the principles of protection of personal data in the primary and secondary education."

More on: http://www.dzlp.mk/en/node/2194

SIN – Software for Inspection Supervision

Software solution started to be used in 2011, when preconditions were created for the implementation of electronic processing of inspection. With this software, through broad-clear Internet connection that can be used outside the premises of the Directorate contributed towards efficient and economical conduct of the inspection procedure, generating reports (including data for this report) and planning the inspection supervision. Part of the inspection documentation is entered/developed on the spot when inspecting, thus reducing some of the costs, and time consuming as well required for treatment and increases the efficiency of inspectors. The software is designed according to the specific needs of the inspectors of the Directorate, and is in function to generate documents and reports based on previously entered answers upon given

questions. During 2013, through the installation of new modules, by setting new configurations in the system (SIN) series of improvements were made as well in direction of more efficiently generating statistics for making quantitative analysis and data from inspection supervisions performed. New opportunities and mechanisms for treatment and ongoing updating of data were introduced, with the main objective - to get immediate insight on the current situation at any time and in an explicit way.

EVENTS

- A new look of the web page of the DPDP www.dzlp.mk launched on 9th of February marking the celebration of **„SAFE INTERNET DAY"**
- **TAIEX event – Workshop on Computer Emergency Response Teams (CERTs) and Personal Data Protection** http://www.dzlp.mk/mk/node/2352
- **TAIEX Workshop** - **European privacy seal** - is a scheme for determining the compliance of new product or service that the companies plan to offer market values, principles and rules to protect personal data specified in the regulations for the protection of personal data.
- **DPDPA Hosts CEEDPA Conference** http://www.dzlp.mk/en/node/2331
- **DPDP Hosts IWGDPT** http://www.dzlp.mk/en/node/2355
- **Joint on-line inspection performed with colleagues from Bulgaria**

Annual Report 2013 published http://www.dzlp.mk/sites/default/files/u4/Annual_Report_2013.pdf

TRAINING FOR CONTROLLERS AND PROCESSORS

The DPDP has organized a total of 40 training under the Training Program for controllers and processors as well as additional interest shown by controllers 1255 participants were involved. The areas on which trainings were conducted trainings were: brokers and insurance, telecommunications, accounting, dentistry, pharmacy.

INSPECTION

Legislative changes have made organizational, institutional and substantial strengthening of the inspection function of the Directorate. Simultaneously, the commitment of the Directorate is giving emphasis on the preventive role of supervision by introducing so-called check lists (lists of checking) that performs preventive alignment of the acts of the controllers with the Law on Protection of Personal Data. The introduction of check lists is done by regular supervision of self- evaluation of the controllers. The inspection supervisions are performed according to an annual plan and monthly plans which for the reporting period included areas of judiciary, health,

education, banking, telecommunication, pension funds, state bodies, employment agencies. Inspection supervision was performed at 163 controllers and 2 of them were performed upon previous request for determination of breach of the right of personal data protection submitted by natural persons.

Type of inspection	Number of inspections
Regular	161
Incidential	2
Control	-
Total:	**163**

Detected violations and findings whilst inspection supervision performed:

The analyzes of the results of inspections conducted in 2013 found the following common conditions and inconsistencies in the application of regulations to protect personal data in the following areas:

1. **Judiciary - made slow progress** due to failure to meet the criteria for application of technical and organizational measures to ensure confidentiality and protection of personal data; in 2013 at controllers it was established inconsistent application of regulations on data privacy in publication of personal identification number of citizens by executors in the country; for the needs of the employment unfairly and illegally is collected and process personal data of employees from criminal record certificates and are processed personal data of employees by keeping photocopies of their IDs in work files;
2. **Wholesale and retail - made limited progress** because of improper application of technical and organizational measures to ensure confidentiality and protection of personal data processing;
3. **Tourism and restaurants- made some progress** due to failure to meet criteria for technical and organizational measures to ensure confidentiality and protection of personal data processing; inappropriate video surveillance which includes: having no notification for video surveillance, video surveillance outside space sufficient to fulfill the purposes for which it is set, recordings made in video surveillance are kept within which is longer than 30 days, retention and photocopying the document ID (identity card or passport) of the guests without legal basis; the employment procedures require applicants photography, do not take measures for the realization of the rights of subjects of personal data (information access and correction of personal data).

4. **Textile industry/Apparel - made modest progress** for criteria and application of technical and organizational measures to ensure confidentiality and protection of personal data processing; inappropriate video surveillance which includes: having no notification for video surveillance, video performance surveillance outside space sufficient to meet the purposes for which it is set, no rulebook on video surveillance, unfair and unlawful processing of personal data of employees by keeping copies of their IDs in work files.
5. **Media - no further progress** - and still not meet the criteria for application of technical and organizational measures to ensure confidentiality and protection of personal data processing - the publication of certain news on Web location does not perform proper anonymization of personal data of the subject of personal data; media do not comply with the regulations for the protection of personal data in the country.
6. **Health - made good progress** with meeting the criteria for application of technical and organizational measures to ensure confidentiality and protection of personal data processing;
7. **Accounting - made initial progress**, there is still inadequate application of technical and organizational measures to ensure confidentiality and protection of personal data processing;
8. **Prosecution - made good progress** but there is no implementation of criteria for application of technical and organizational measures to ensure confidentiality and protection of personal data, no acts are adopted and applied that set limits on storage of documents containing personal data and no destroying documents that contain personal data is made, for which the storage period has expired and the purpose for which they were collected is fullfilled. However, it is considered a major advance in the field, the submission of the first national report to Eurojust on the state of affairs at Public Prosecution in Macedonia regarding the application of the regulations to protect personal data.
9. **Employment - made further progress**, but it is necessary to follow the criteria for application of technical and organizational measures to ensure confidentiality and protection of personal data processing, there is inconsistency in the collection, processing and storage of personal data relating to applicants and which is not in accordance with law, as well as incomplete, inaccurate and out of date data.
10. **Construction - made unsatisfactory progress** in terms of inconsistent application of technical and organizational measures to ensure confidentiality and protection of personal data processing; inconsistency of regulations to protect personal data when processing by storing a copy of the identity card of the employees in their working files; inappropriate video surveillance outside space which is sufficient to fulfill the purposes for which it is set.

11. **Banking - made significant progress**, however, special attention should be paid to excessive processing of personal data in applications for various types of loans, as well as unfair and unlawful processing of personal data of employees by copying and keeping a copy of their ID card in the work files.
12. **Education -** although **significant progress has been made** - this area needs to meet the set criteria for the application of technical and organizational measures to ensure confidentiality and protection of personal data processing; simultaneously, improperly performing video surveillance which includes video surveillance from space which is sufficient to fulfill the purposes for which it is set.

Complaints - In the reporting period, there are 227 complaints and proposals from natural and legal persons in the following areas:

Area	Number
Social networks	149
State bodies	19
Banking/Economy	6
Judiciary	1
Education	5
Health	1
Electronic communications	11
Direct marketing	1
Energetics	2
Labor	5
Cadaster	2
Video surveillance	8
NGO	1
Tourism	1
Trade	2
Public services	3
Housing	1
Media	4

Post services	2
Lottery	1
Statistics	1
Internet	3
Total	**227**

INTERNATIONAL COOPERATION

DPDP Representatives continuosly are present on the Working Group 29 and the Spring Conference meetings, the Conference of the European Authorities for Personal Data Protection. EUROJUST and - in accordance with the provisions of Article 17 of the Law on Ratification of the Agreement on Cooperation between Macedonia and EUROJUST the Directorate for Personal Data Protection in the Republic Macedonia shall report annually on the situation in the judiciary in relation to the implementation of the regulations on the protection of personal data. On this basis the DPDP performed inspection in all Public Prosecution Offices in the country and on that basis prepared and submitted to EUROJUST for the first time the first National Report. The purpose of this report is to present the actual state of public prosecutions in the country in terms of implementation of regulations for the protection of personal data processing.

LEGISLATION

The Directorate for Personal Data Protection has actively participated in the adoption of the new Law on Criminal Procedure[4] and has issued opinions on delivery of different sectorial laws.

Recent national developments

Introducing **E- SERVICES** - Current situation in state bodies and institutions indicates that only a certain number of electronic services offered to citizens and business community. Electronic services significantly decrease time and facilitate economic way of getting service users and they have proven to be efficient and effective way of getting the service. The concept of e-services provides any interested IT company to meet certain technical and legal requirements

[4] Law on Criminal Procedure („Official Gazette of the RM“no.150/2010 and 100/2012), entered into force on December 01, 2013.

and standards to be developed to allow IT solutions that will offer electronic services, using the registers of the institutions through strictly defined rules and standards.
Ongoing activities for **E- TRADE** – Activities are under to encourage and facilitate electronic commerce to stimulate electronic commerce as a tool for economic development in Macedonia.

DIGITAL CERTIFICATES - This project provides for the promotion of the benefits of using digital certificates by accredited certificate for all employers who have a legal obligation to report and pay taxes in order to enable them to electronically submit documents to state institutions and going to minimize their desks. This will facilitate and promote the use of current and future electronic services such as: Electronic publication of social security contributions and personal income, Electronic tax return, Electronic publication of annual accounts, electronic banking, electronic payment of taxes and other payments, electronic public procurement (digital certificates are mandatory from 1 January 2008), electronic registration of employees in the Employment Declaration for Electronic import - export etc.
Will be identified and removed obstacles to the appointment of CA (Certificate Authority) and will support the use of electronic documents and signatures in domestic and cross-border trade and communication with state institutions.

OPTICAL GOVERNMENT IT NETWORK -Ministry of Information Society and Administration introduced optical Government IT network, which allows achieving higher speeds of data transmission, greater security of transmitted data and the growing number of electronic services to citizens. The implementation of country optic communication network in the future will entail reducing the financial costs of renting expensive internet links. Its implementation will enable expansion of more vital projects that increase accuracy, quality and quantity of services that use state institutions to work every day. The project cost a total of eight million of the passive and active equipment, and performed in collaboration with the Ministry of Interior and the Macedonian Telecom. The successful implementation of this project should lead to a reduction in financial expenses allocated to connect to internet and fixed telephony in all state bodies. The space will allow for the implementation of new IT projects, such as the introduction of Internet telephony (Voice over Internet Protocol), a centralized system for managing documents (Document Management System) in all institutions, interoperability between all institutions participating in the issuance relevant documents or in any way provide services to citizens or companies. Otherwise, with this system are linked to a total of 24 institutions in the country: The General Secretariat of the Government of the Republic of Macedonia, Secretariat for framework agreement, Secretariat for European Issues, the ministries, the Government of the Republic of

Macedonia, the joint IT center, the Parliament of the Republic of Macedonia, the Customs Administration, the Public Revenue Office, Administration for keeping the population register, MarNet - system matrix and the Office of the President of the Republic of Macedonia.

GOOGLE STREET VIEW – DPDP involved in preoperational phase of introducing it in Macedonia –

In April this year a meeting was held for the preparatory activities for introducing it in the country.

UKRAINE

Within realization of Ukraine's obligations concerning the ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and 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, Ukraine undertakes measures to improve the system of personal data protection and to bring it into compliance with the Council of Europe and the EU standards.

On 1 January 2014 the Law of Ukraine “On amendments to certain legislative acts of Ukraine concerning the improvement of the protection of personal data”, which amends the Law of Ukraine “On the protection of personal data”, came into force.

According to these amendments the function of control over observance of the legislation on protection of personal data is assigned to the Ukrainian Parliament Commissioner for Human Rights (hereinafter referred to as the Ombudsman). This measure complies with requirements of international documents concerning the independence of the national supervisory authority, that is responsible for ensuring compliance with legislation for the protection of personal data.

In the field of personal data protection Ombudsman has the following powers : consideration of complaints and appeals; inspection of personal data controllers and/or processors; submission of proposals for the elaboration of personal data protection policy; approval of legal acts on personal data protection, interaction with subjects of foreign relations related to personal data issues etc.

Based on inspections and appeals Ombudsman may issue requests on elimination of violations of the legislation on data protection. These requests are obligatory for controllers. In addition, Ombudsman has the right to draw up records on bringing to administrative responsibility and send them to the court in cases envisaged by the law.

In pursuance of articles 9 and 24 of the Law of Ukraine “On the protection of personal data” on 8 January 2014 by order of the Ombudsman the list of legal acts was approved:

- Model Procedure for processing of personal data;
- The procedure for monitoring compliance with personal data protection legislation;
- The procedure for notification of the Ombudsman of processing of personal data which pose a severe risk to the rights and liberties of subjects of personal data and about departments or responsible person who organizes the work related to the protection of personal data during their processing and the procedure for publication of information that was mentioned. This procedure defines, among other things, a list of "sensitive" personal data.

For the purpose of effective realization of powers in the field of protection of personal data the Ombudsman has established the position of Representative of the Commissioner for Personal Data Protection. Besides, the Department for Personal Data Protection was established in the Secretariat of the Ombudsman. The main task of this Department is to ensure the exercise of powers of the Ombudsman in the field of personal data protection, including the monitoring of the observance of human rights to the protection of personal data, consider citizens' complaints and undertake measures to restore their rights to personal data protection.

On 13 May 2014 Verkhovna Rada of Ukraine adopted the Law “On amendments to laws of Ukraine connected with the work of Ombudsman in the sphere of personal data protection”, which was elaborated in order to complete the first (legal) phase of the Action Plan for liberalization of visa regime for Ukraine by the EU in the field of personal data protection.

Currently the Law of Ukraine “On the Ukrainian Parliament Commissioner for Human Rights” defines the powers of the Ombudsman only in relations arising from the fulfillment of human and citizens' rights and freedoms only between a citizen of Ukraine, irrespective of his or her dwelling place, a foreigner or a stateless person, who are on the territory of Ukraine and bodies of state power and local self-government, their officials. According to amendments that were adopted on 13 May 2014 the scope of application of the Law of Ukraine “On the Ukrainian Parliament Commissioner for Human Rights” shall extend to relations arising between legal entities of public and private law and natural persons on the territory of Ukraine.

This Law also introduces to the Law of Ukraine “On the protection of personal data” definition of personal data subject’s consent.

In addition, the Law regulates the institutional aspect of personal data protection in such laws of Ukraine as “On the State register of voters”, “On the collection and accounting of a single fee for obligatory state social insurance”, “On the unified state demographic register and documents certifying the citizenship of Ukraine, personal identity or her/his special status”.

AUSTRALIA

Recent major privacy developments in Australia

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia
on behalf of the Australian Privacy Foundation (International Committee) – 22 May 2014

Prepared for Council of Europe Convention 108 Consultative Committee, 31st Plenary Meeting, item V.

Abolition of the Australian Information Commissioner

In May 2014 the new federal Coalition government, in its first Budget, abolished the positions of Australian Information Commissioner and Freedom of Information Commissioner, and the Office of the Australian Information Commissioner (OAIC), as part of a broader abolition or merger of many federal agencies. The Privacy Commissioner's office had been merged with the new OAIC in November 2010, and (in summary) the Privacy Commissioner made subordinate to the Information Commissioner. The response of the three Commissioners explains how freedom of information law will now be administered, and what they consider to be OAIC's achievements.

After the new changes become operational in January 2015, the Privacy Commissioner will, as a separate statutory officer, take back full responsibility for the *Privacy Act 1988*, with an office co-located with the Human Rights Commission (HRC). It remains uncertain whether the Privacy Commissioner will share staff with the HRC, or become a member of the HRC, both of which were once the case. The incorporation of the Privacy Commissioner into the Information Commissioner triumvirate had produced few obvious benefits to privacy protection since 2010, but whether the Privacy Commission will be given adequate resources under the new arrangements is very doubtful.

See AIC 'Australian Government's Budget decision to disband OAIC' <http://www.oaic.gov.au/news-and-events/statements/australian-governments-budget-decision-to-disband-oaic/australian-government-s-budget-decision-to-disband-oaic>

New enforcement powers in Privacy Act 1988, from March 2014

On 12 March 2014 amendments to the *Privacy Act 1988* came into force. They are the most substantial changes since most of the private sector was included within its jurisdiction in 2011. Enforcement powers under the Act have been strengthened greatly, including civil fines potentially up to A$1.6 million. For the first time, there is a right of appeal against decisions (determinations) by the Privacy Commissioner to the Administrative Appeals Tribunal. However, it will be of little use while the Commissioner continues to make on average less than one determination per year against which an appeal may be lodged. The privacy Principles, are weakened, not strengthened.

Law reform enquiry into ‘serious privacy invasions’ (tort/civil action)

Australia does not have a tort (civil action) for privacy protection, and nor can breaches of the Privacy Act be taken directly to the courts. The Australian Law Reform Commission has a reference from the previous (Labor) government to examine whether there should be a statutory action for ‘serious invasions of privacy’. It has produced a discussion paper, and will report by July.

Mandatory data breach legislation again before Parliament

A Bill to require mandatory data breach notification was supported by all parties in the 2013 Parliament but not passed in time. It has been re-introduced into the 2014 by the Greens.

For details of these three items, see G Greenleaf ‘Australia’s privacy enforcement strengthens, but gaps in appeals and transparency remain’ (2014) 128 *Privacy Laws & Business International Report* 1-5 (copy attached)

MEXICO

MAJOR DEVELOPMENTS IN DATA PROTECTION IN MEXICO
OCTOBER 2013-MAY 2014

Introduction

This paper reports on the major developments of the Federal Institute for Access to Information and Data Protection (IFAI) regarding the protection of personal data, for the period October 2013 - May 2014[5].

The document is divided into the following sections: I) introduction, II) IFAI powers for the protection of data, III) regulatory developments, IV) prevention, outreach and compliance, V) procedures, and VI) IFAI's international participation.

I. Introduction

In Mexico, the fundamental right to the protection of personal data is recognized in Article 16 of the Constitution of the United Mexican States (the Constitution) and is regulated by various statues, both federal and state. This fundamental right is regulated for the public and private sectors.

The statutes that regulate the processing of personal data in the **public sector** are:

- At federal level, the Federal Law of Transparency and Access to Public Government Information (LFTAIPG), and
- At the state and municipal level, the various state laws.

For the **private sector,** the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) is the regulation which governs the processing of personal data throughout the national territory.

The guarantor of the right to the protection of personal data for the federal public sector is the IFAI –which is also the guarantor of the right of access to information–, and, at the state level, each state has a similar body to guarantee the protection of these rights before local public entities. Moreover, IFAI is the only authority for the processing of personal data in the private sector.

It is worth mentioning that, until today, at the federal level, the executive branch, the judiciary branch and the autonomous constitutional bodies have their own entities to ensure the right to the protection of personal data.

II. Powers of IFAI on data protection

Currently, in terms of the LFTAIPG and the LFPDPPP, IFAI has the following powers:

[5] The figures are as of April 30, 2014.

- **Regulatory Powers:** it interprets the LFPDPPP and the LFTAIPG, as well as their regulations; gives opinions and recommendations to ensure the full protection of personal data; and disseminates international standards and best practices in the field.

- **Information Powers**: provides technical support to regulated parties of both laws that request it, in order to support them to comply with their obligations; develops and disseminates discussions, studies and research on the subject. By law, IFAI is required to submit an annual activity report to the Congress.

- **Surveillance Powers:** oversees and verifies compliance with the provisions contained in the law and prepares impact studies on privacy prior to the implementation of a new form of processing of personal data or substantial modifications to existing processing methods.

- **Adjudicative Powers:** in the private sector, hears and resolves procedures on rights protection and verification, and imposes sanctions as appropriate. Cooperates with other supervisory authorities, as well as domestic and international data protection agencies.

- **Sanctioning Powers:** the LFPDPPP sets forth a range of behaviors considered violations and their corresponding penalties, ranging from warning to imposing maximum fines, under a system of modulation of the penalty, according to the seriousness of the behavior.

III. Regulatory Developments

- **Constitutional Reform:** Mexico is in the process of adapting legislation on access to information and protection of personal data. With the reform of Article 6 of the Constitution (February 7, 2014), the legal nature of IFAI and its powers changed; the list of regulated parties was expanded, and a solid institutional framework was created to fully guarantee these fundamental rights.

  IFAI is constituted as an autonomous constitutional body and, by amending the laws of the respective subjects[6] it will be:

  - With regard to personal data in the public sector:
    - Authority for the Executive, Legislative and Judicial Branches (except the Supreme Court of Justice) and the Constitutional Autonomous Bodies, political parties, etc.; and
    - Second instance regarding remedies in state oversight bodies.

  - With regard to personal data in the private sector:
    - It shall remain the guarantor body.

  - The ***Guidelines of the Privacy Notice*** and ***Parameters for the proper development of self-binding schemes referred to in Article 44 of the Federal Law on Protection of Personal Data Held by Private Parties*** were published in 2013, which develop the model of self-regulation in the matter, provide for minimum and facultative contents for self-binding schemes, and develop the main features of the certification system in the field.

[6] The constitutional reform established a one-year term to make the necessary legal adjustments.

- On October 30, 2013 the ***Recommendations on Personal Data Security*** were published.

- In 2013, the **Operating Rules for the Registration of the Binding Self-Regulating Scheme (REA)** were developed, which were adopted on October 9, 2013. These include operational and procedural aspects of the proceedings of the binding self-regulatory schemes and of accreditation bodies before IFAI. On October 18, 2013 the website www.rea.ifai.org.mx was made publicly available, where one can search information for self-regulation on the protection of personal data, included in the certification system, and the REA.

IV.

Prevention, outreach and compliance

- **Advice:** citizen service modules provide advice to the regulated parties by the LFPDPPP and its Regulations, clarifying questions about the rights and obligations to be observed in the treatment of personal data. Between October 2013 and April 30, 2014, around 498 cases on personal data were handled.

- **Personal Data Protection System / Case Manager System (PRODATOS):** an electronic system was designed that facilitates citizens submitting applications for protection of rights or claims via the Internet, within the LFPDPPP framework. In the first week of operation (March 2014), there were 1,384 visits to the site and 215 users were registered. Through this means, 12 complaints were received, and 22 are under development and delivery through the portal.

  - In 2013, ***The ABC of the Privacy Notice*** was published. This is a guide describing the steps to generate a privacy notice, the data elements it must contain, and develops models of privacy notice. Likewise, a model of ***privacy notice for video surveillance,*** and the ***privacy notices self-assessment form*** were published, the latter aimed at all those responsible for data processing. In October 2013, the ***Guide to implement a Safety Management System of Personal Data,*** and the ***Risk Analysis Methodology*** **BAA** were published. In November 2013, the ***model of simplified privacy notice in video format*** was made available at IFAI's portal. In March 2014, the ***Manual on security of personal data for MSMEs and small organizations*** was prepared. In April 2014, ***Models of Privacy Notices for Migrants*** were developed.

  - In September of 2013 the ***Generator of Privacy Notices*** (GAP) was launched. This is a software tool available in the www.ifai.org.mx webpage, through which one can create free privacy notices, with the elements required by the standard. The GAP was developed by the Institute and will enable all those responsible for the processing of personal data to be updated with the issuance of the Privacy Notice obligation under the LFPDPPP. Between October 2013 and May 2014, 30,406 Privacy Notices were created.

- **International Day for Data Protection:** On January 28, IFAI joined the International Day for the Protection of Personal Data, institutionalized in 2006 by the Council of Europe. Its purpose was to promote the exercise of the right to protection of personal data on two

fronts: first, from the perspective of the owners, as a fundamental right, and second, from the point of view of those responsible, as to LFPDPPP compliance. IFAI organized events in eleven cities in Mexico (Guadalajara, Torreón, Veracruz, Mérida, León, Monterrey, Tijuana, Pachuca, Villahermosa, Oaxaca and Tlaxcala).

- **Questions addressed:** between October 2013 and April 30, 2014, 391 specialized queries were received in the following areas: 233 (59.6%) privacy notices; 148 (37.8%) on various issues regarding the protection of personal data; and 10 (2.6%) of binding self-regulatory schemes.

- **C**

  ollaboration Agreements. IFAI has entered into cooperation agreements with 12 chambers and associations to disseminate the right to data protection, technical advice to the associated partners and the creation of working groups in the field. Until April this year, there had been 48 workshops, in which approximately 1,200 executives were trained.

V. Law Enforcement

The laws governing the right to protection of personal data contain procedures that are aimed at ensuring the proper exercise of this right. IFAI addresses the following:

- Regarding the LFTAIPG, regulating those responsible from the public sector:
  - Review Remedies
  - Verification
- Regarding the LFPDPPP, which regulates the private sector:
  - Verification Procedure
  - Rights Protection Procedures
  - Procedure for Imposing Sanctions

During this period, the following procedures have been carried out:

Review Remedies. This procedure is a means to submit disagreements to the responses that regulated parties by LFTAIPG in the **public sector** provide with respect to the exercise of ARCO rights. In this period, 17,524 applications have been submitted to the Federal Executive Branch for the exercise of ARCO rights. Of these, 865 procedures have been initiated for review and 895 were resolved[7], pending resolution of a total of 156 as of April 28.

Rights Protection Procedures This procedure is a means to make claims for disagreement with the answers that the regulated parties of LFPDPPP provided on the exercise of ARCO rights in the **private sector,** or for lack of response to requests for exercise of ARCO rights. In this period, 62 applications were received relating to rights protection and 47 resolved, pending resolution 15. A feature of this method is that it supports the conciliation of the parties, which significantly speeds up the exercise of this fundamental right. During this period, 12 cases have been reconciled. However, if during the course of the procedure it is found that the responsible

[7] This figure includes procedures resolved during the reporting period and which had been initiated previously.

party has committed an offense, IFAI orders to begin a a process of imposing sanctions. In the period reported, this occurred on 4 occasions.

The laws empower the Institute to conduct **research and checks** that allow verifying their compliance, and of the regulations derived therefrom. In this sense, during this period 170 investigations were initiated in the public sector and 124 were completed. Likewise, 14 checks to the private sector were initiated and 11 completed. From these checks, all of them gave rise to sanctions procedures. In the reporting period no checks were carried out the public sector.

The last procedure is the **imposition of sanctions.** The LFPDPPP sets forth a list of behaviors that are considered violations and deserve to be penalized. The fine is the most common penalty; however, a warning can also be imposed for the responsible to perform the acts required by the holder. In this period, 16 procedures were initiated and 10 completed and fines imposed totaling $ 1.8 million US dollars.

VI. International participation of IFAI on data protection matters

The Institute has taken the following actions with international impact:

2013	Mexico is accepted as an member economy in the APEC Cross-Border Privacy Rules System
	Mexico's interest to adhere to Convention 108 of the Council of Europe (CoE) was confirmed
	General Cooperation Agreement between the Spanish Data Protection Agency and the IFAI
	At the 35th International Conference of Data Protection and Privacy Commissioners (Warsaw, Poland, 23-26 September), IFAI cosponsored four resolutions
	In December, IFAI organized the International Forum on the security of personal data
2014	IFAI participates for the first time in the *Privacy Sweep*, an activity organized by GPEN .

UNITED STATES OF AMERICA / ETATS UNIS D'AMERIQUE

The White House's report on big data and privacy:

http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Report of the President's Council of Advisors on Science and Technology on big data:

http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

URUGUAY

Summary of the development of Data Protection regulations in Uruguay

Act No. 18.331 on the Protection of Personal Data and “Habeas Data” Action, which was proclaimed on 11 August 2008, expressly acknowledges the existence of this right, as inherent to the human being, which is included in article 72 of the Constitution.

The control authority for data protection, called "Unit for the Regulation and Control of Personal Data" (URCDP in Spanish), was created by virtue of section 31 of the aforementioned Act. It is an entity with the very broadest technical autonomy, as well as with specific duties and powers.

This act was supplemented by two regulatory decrees. Decree No. 414/009 of 31 August 2009 was adopted to clarify some aspects of this Act, as well as to lay down detailed regulation concerning the organization, powers and functioning of the Data Protection Control Body. Decree No. 664/008 of 22 December 2008 refers to the regulation of registration procedures of databases which provide objective commercial information.

Over time, and aiming to improve the system which protects this human right, the URCDP promoted some amendments to Act No. 18.331. In this regard, Act No. 18.996 of 7th November 2012, incorporates article 9 bis, which set forth the scope of the concept of public sources according to this Act.

On October 2012 it was held the 34th International Conference of Data Protection and Privacy Authorities in Punta del Este. At the same time, it was held the Ibero-American Data Protection Network (RIPD in Spanish) meeting, as well as other "simultaneous events" organized by representatives of the civil society and academia.

The open sessions of this conference, which were organized by the URCDP, consisted of different panels entitled "Privacy and Technology in Balance". Thus, our country hosted a highly importance meeting regarding the issues considered, the activities carried out, as well as the relevant people who attended from every continent.

On the other hand, on 21 August 2012, the European Union, through its competent bodies and according to Directive 95/46/EC of the European Parliament, considered that our country "ensures an adequate level of protection with regard to the processing of personal data and the free movement of such data".

This implies the EU recognition of the adequacy of the Uruguayan system on data protection to the best international standards. In this regard, apart from the implications related to data exchange with Europe, which currently does not demand specific requirements (models of contractual clauses, binding corporate rules, etc.) it has had an immediate impact on the country, which may be observed by the increase on the queries submitted to the Unit.

Accordingly, during 2012 the Legislative Branch passed Act No. 19.030, which was enacted by the Executive Branch on December 27. This Act enables the accession of Uruguay to Council of Europe Convention No. 108, of 28 January 1981, for the Protection of Individuals with regard to Automatic Processing of Personal Data, and its additional protocol.

The Uruguayan system of data protection is further strengthened over time in order to respond to the changing society. Article 75 of Act No. 19.149 (Rendering of Accounts and Balancing of Budget Execution, Exercise 2012, of 24 October 2013) states that mobile telephone service providers shall keep updated records of their customers who have hired services under any type of contract, either prepaid or postpaid. This Act also provides that this database shall be covered by Act No. 18.331 of 11 August 2008.

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

- Depuis la précédente réunion plénière, adoption en novembre 2013 par l'association des autorités de protection des données de la francophonie de trois résolutions : sur la transparence des pratiques des gouvernements en matière de renseignements ; sur l'éducation au numérique pour tous ; et sur l'encadrement des transferts de données dans l'espace francophone au moyen de règles contraignantes d'entreprises ;

- Publication d'un guide pratique inédit pour la consolidation de l'état civil, des processus électoraux et la protection des données personnelles le 20 mai (demain) ; ce guide soutenu par l'OIF aborde la question de l'usage de l'informatique et de la biométrie sous l'angle de l'impératif de modernisation et de démocratisation des Etats et de protection des données personnelles ;

- Lancement d'une action collective pour inscrire la protection des données à l'agenda du sommet de la Francophonie à Dakar ;

 ACTIONS/DOCS QUI CONCERNENT/PEUVENT CONCERNER PLUSIEURS PAYS MEMBRES DU COE. BESOINS DE RELAIS NATIONAUX ET DU SOUTIEN DU COE.

- 8ème conférence francophone à Ouagadougou les 22 et 23 septembre 2014 ; conférence en français ouverte à la participation des autorités, des Etats et des organisations partenaires telles que le COE ; les éléments du programme pourront être présentés le 4/6 juin ;

- Se féliciter de la participation de 5 pays non membres du COE, africains, francophones, aux réunions du CAHDATA ; montre le résultat des efforts de promotion de la Convention 108 dans l'espace francophone, en particulier en Afrique ; se féliciter et remercier le COE pour les 2 séminaires organisés en Tunisie et au Maroc en mars 2014.

EUROPEAN DATA PROTECTION SUPERVISOR / LE CONTRÔLEUR EUROPEEN DE LA PROTECTION DES DONNEES (EDPS)

EN version of the April 2014 newsletter:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_41_EN.pdf

EN version of the December 2013 newsletter:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_40_EN.pdf

Newsletters page of our website:

https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Newsletters