COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 22 June / juin 2016

T-PD(2016)10Mos

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

ARMENIA / ARMENIE 11

AUSTRIA / AUTRICHE 12

BELGIUM / BELGIQUE 13

BOSNIA AND HERZEGOVINA / BOSNIE ET HERZEGOVINE 16

CROATIA / CROATIE 18

CYPRUS / CHIPRE 19

CZECH REPUBLIC / REPUBLIQUE TCHEQUE 20

DANEMARK / DENMARK 21

FINLAND / FINLANDE 22

GEORGIA / GEORGIE 24

GERMANY / ALLEMAGNE 26

ITALY / ITALIE 28

ICELAND / ISLANDE 31

IRELAND / IRLANDE 33

LIECHTENSTEIN 36

LITHUANIA / LITHUANIE 37

MALTA / MALTE 39

MONACO 41

POLAND / POLOGNE 43

SLOVENIA / SLOVENIE 50

UKRAINE 55

UKRAINE - MEDIATRICE DE L'UKRAINE 57

URUGUAY 61

EUROPEAN DATA PROTECTION SUPERVISOR / LE CONTRÔLEUR EUROPEEN DE LA PROTECTION DES DONNEES (EDPS) 62

INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) 66

ALBANIA / ALBANIE

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD
"July 2015-June 2016"

INFORMATION AND DATA PROTECTION COMMISSIONER OF ALBANIA

- **Activity in implementation of the law on personal data protection**

  - *Sub-legal acts approval*

The Instruction No. 43, dated 09.02.2016 was approved "On some addenda and amendments in the Instruction No. 21, dated 24.09.2012 "On determining rules on safeguarding personal data processed by large controllers", as well as **the Decision No. 7, dated 09.02.2016** "On some amendments in the Decision No. 3, dated 20.11.2012 "On determining states with adequate level of personal data protection". The amendments are initiated by the recommendations provided by EUROJUST in the framework of the Cooperation Agreement to be signed with this agency.

  - *Other legal framework developments*

In some draft laws (not approved yet) additional powers are provided to the Commissioner to approve instructions in certain sectors. This form shall influence the role and monitoring and supervision work of the Commissioner to fair and legitimate data processing by the controllers.

In the draft-law "On additional security measures" the Commissioner is provided with the power to approve a sub-legal act (instruction) "*On determining the level of security measures during the processing of data by CCTV*" and monitoring its implementation.

In the draft-law "On Electronic Commerce", the Commissioner is provided with the power to approve a sub-legal act (instruction) "*On determining detailed rules regarding the exemptions register by unrequested communications by the service recipients, natural persons*", the monitoring and addressing several categories of complaints.

In the draft-law "On whistleblowers", the Commissioner is provided with the power to approve a sub-legal act (instruction) "On determining conditions, criteria and time of retention of personal data in the field of whistleblowers".

In the draft-law "On cross-border control", the Commissioner has a common power with the Minister of Interior to approve a sub-legal act (instruction) "*On determining rules of administration of data collected during the cross-border control*".

  - *Opinion provided for sub-legal and legal draft/acts*

The Commissioner's Office aimed to foster private and public entities to provide opinion to for any legal and sub-legal draft law, various legal documents, agreements, etc, related to the field of personal data protection. In this regard, every meeting, reporting, training or even public opennes is exploited.
In this reporting period 37 b/laws and sub-legal draft laws are addressed for opinion.

Some of them are mentioned below:

Draft law "On some addenda and amendments in the Law No. 7961, dated 12.07.1995 "Labour Code of RA" as amended, sent by the Assembly of the Republic of Albania.

Draft law "On one addendum in the Law No. 7895, dated. 27/01/1995, "Penal Code of the Republic of Albania ", as amended".
Draft law "On Electronic Commerce"
Draft law "On some amendments to the Law no 53/2014 "On deposits insurance", sent by the Ministry of Finance.
Draft law "On some addenda and amendments to the law no 10128, dated 11.5.2009 "On electronic commerce", as amended, sent by the Ministry of State for Innovation and Public Administration.
Draft law "On whistle-blowers", sent by the State Minister for Local Issues.
Draft law "On the registration of the address of the Albanian citizens living outside the territory of the Republic of Albania", sent by the Ministry of Interior.
Draft law "On border control", sent by the Ministry of Interior.
Draft law "On the organisation and functioning of the local governance", sent by the State Minister for Local Issues.
Draft decision "On the approval of the "Regulation on electronic identification and trusted services" sent by the Ministry of State for Innovation and Public Administration.
Draft decision "On the approval of the rules for the establishment and administration of the electronic register for public notifications and consultations", sent by the Ministry of State for Innovation and Public Administration.

- *Cooperation agreement*

IDP has marked achievements in the context of inter-institutional relations. During this period, several cooperation agreements were signed by the Information and Data Protection Commissioner.

Cooperation Agreement between IDP and AMA

On 23 September in the Premises of the Commissioner, the cooperation agreement was signed with the Authority of Audio-Visual Media. This document is a sound base for coordinating the efforts between both authorities in the process of monitoring and implementing the legal acts in the respective fields and in mutual cooperation. The agreement attaches specific importance to processing the personal data of citizens by media in compliance with the provisions of the respective law, however, it also induces them to assume the right for information in a balanced fashion

Cooperation Agreement between IDP and NRC and between IDP and NLC

The Information and Data Protection Commissioner signed up two cooperation agreements, respectively with the National Registration Centre and the National Licensing Centre. These documents define clear modalities for coordinating the efforts between the Office of Commissioner and the NRC and NLC in the process of monitoring the implementation of legal acts in the respective fields.

- *Fulfilling obligations in the context of 2015 Progress Report*

In the progress report is cited among others that, … *the Media often violates the right to protection of personal data….*

In order to minimize this issue, the Commissioner's Office considered as important the signature of the cooperation agreement with the Audiovisual Media Authority (metioned above).

Prior to sign the cooperation agrement and in the following, the Commissioner's office has negotiated with stakeholders that operate in the field of media as AMA, ISHM and Association of Journalists to conduct joint activities aiming to raise awareness in the field of media on the protection of personal data. 2 meetings were conducted following this reporting period.

Several complaints were addressed related to the disclosure of personal data in the media through which, the Commissioner's Office has informed the controllers (media) to respect privacy.

Currently, following by the close cooperation with the media authority, as well as by compliants being addressed in relation to the media, it is noted that this authority has inter-acted regarding to handling cases.

In this progress report is also stated *(Chap. 23, Judiciary and fundamental rights pg. 54) online access of jurisprudence is not fully guaranteed and does not have an accessible database. Court rulings are not systematically published; when published, the justification is not always contained and deadlines are not always respected. Efforts are needed to improve drafting skills of judges. Publication of court decisions anonymously is not possible yet.*

In this context, the obligations of judicial bodies to acomplish this purpose, remains unfulfilled yet. Meanwhile the Commissioner is evaluating the possibility to amend fully or partly the instruction no. 15/2011 "On the processing of personal data in the judicial system", to facilitate its implementation and adapt it with provisions of the law 119/2014 "On right to information".

- **The fulfillment of the controllers' main obligation, carrying out the notification**

In this regard, as first step, which is assessed with expectations is the intensive continuation of the awareness process of the processing and controlling subjects, acquaintance with the Law No. 9887, dated 10.03.2008 "On personal data protection", as amended, as well as the implementation of the legal obligation to notify at the Commissioner's Office on the status of the processing of personal data.

- ***Management of notifications and registration of controlling subjects/ May 2015 – May 2016***

As a result of the awareness strategy, but also legally binding, during this period at the Commissioner's Office **460** controlling subjects have notified, by which **5** non-profit organizations, **41** public subjects and **414** private subjects, following with an overall number of notifications to **5217**. It's been followed with registration and online publication in the Opened Register to Public of notifications that result to carry out the processing of personal data In conformity with Articles 5 and 6 of the Law No. 9887, dated 10.03.2008 "On personal data protection", as amended.
The number of controlling subjects registered for this period is **456**, following with an overall number of the registered subjects in the opened register to public in **5163**.

- **Policy and Surveillance Effects**

Accomplishment of controls and administrative inspections at public or private controllers is a continuous engagement of the Commissioner's Office, which aims to guarantee the compliance to the legislation in the field of data protection and guaranteeing the rights of data subjects.

The supervisory role during the reporting period, is successfully accomplished by the Commissioner's Office through the controls, inspections, initiated mainly *(ex-officcio)* or by the complaints of data subjects.

- *Processing the Compaints*

During this period, **90** complaints were lodged at IDP, requests for information and concerns for potential infridgements related to personal data by various controllers (public or private). In order to resolve fairly and fully the complaints, according to the case, administrative inspections are conducted at various controllers and all procedurial steps are followed as a continuous communication with complaining subjects and controllers in the framework of collecting information.

Complaints are focused in:

- Direct marketing, being the highest number of complaints, and mainly on the unsolicited

communications, through the phone or electronic post;
- Publication of the personal data in media and official internet websites of the controllers; Assuming the right of the entities to access for rectifying/deleting the personal data;
- Data processing without the consent of data subject and without carrying out its prior information;
- Illegal disclosure of personal data;

Even in the course of this year, a considerable number of complaints were submitted with the Office of the Commissioner through the electronic mail made available to the entities of personal data info@idp.al. This has put in place a fast and direct communication with the entities, thus facilitating the procedure and duration of the settlement of complaints.

- *Controls and administrative inspections mainly (ex-officcio).*

In enforcement of its surveillance policies, IDP for this period has exercised **127** controls and administrative inspections, thematic and sectorial. Controls and administrative inspections are focused in particular sectors such as:

- Banking sector;
- Marketing sector (call center);
- Health sector;
- Media (inspections on basis of complaints);
- Video surveillance;
- Public Authorities;
- Telecommunication, (the process of deletion of personal data);
- Local government (online inspections and on basis of complaints).

The main purpose of the Commissioner's Office has been the verification of the enforcement of the legislation on personal data protection in certain sectors, encountering issues and providing assistance in the context of implementing and respecting legal obligations.

Moreover, IDP has exercised online inspection also **(48 in total)** conducted in the local government sector (**29**) and the education sector (**19**). These inspections are focused in the processing of personal data in the controllers'website, privacy policies, informing data subjects and the manner of obtaining the consent of data subjects.

Carrying out online inspections is considered as a way to raise awareness of controllers on the importance of respecting rules with regard to privacy, theur obligation to notify data subjects regarding their rights in implementation of the law on personal data protection.

- *Recommendations.*

The Commissioner's Office came out with **35** Recommendations during the administrative investigations exercised, in cases when the foundings have not affected (or by not affecting directly) the privacy of data subjects.

- *Order for prohibiting data processing and destruction of data collected illegaly.*

During the administrative investigations exercised in the halth sektor, it was found that a controller carries out collection and data processing through video surveillance systems (CCTV) in intimate premises. Following by the documentation of the infridgements found, the Commissioner's Office came out with an order, object of which is to prohibit processing of personal data collected through video surveillance system (CCTV) in intimate premises and their deletion in unrecovable manner. The controller has taken measures and documented the implementation of the Commissioner's Order.

- *Administrative Sanctions (Fines)*

In implementation of legal powers, in each case when serious breaches of the law are found and repeated or inconsistency of applying Recomendations and Orders, the Commisioner has imposed sanctions. In total, **53 administrative sanctions** with **fine** are imposed.

Infridgements for which sanctions are imposed, are referred mainly to breaches by controllers, on the obligation to inform of data subject, the obligation in regard to taking measures for safeguarding personal data in contractual agreements with third parties and the obligation related to the completion and updating the "notification form" at the Commissioner's Office. Imposing administrative sanctions is conducted by the Commissioner's Office under the law as well as in respecting the legitimate principles, transparency in decision-making and the rights of parties to be heard. After reviewing the relevant papers, as a result of administrative investigations, in cases where breaches of the law were found, **hearings** were conducted. Hearing sessions took place after prior notifying the controllers and in respect of the right of subjets to be heard pursuant to Articles 93-96 of the Law No. 8485, dated 12.5.1999 "Code of Administrative Procedures of the Republic of Albania" prior to imposing the final decision with fine to the controller.

- *International transfer*

Special attention was assigned to the requests for authorization of the Commissioner for international transfer of personal data in countries without adequate level of protection of personal data, according to the definition in the Commissioner's Decision No. 3, dated 20.11.2012 *"On determining countries ensuring an adequate level of protection of personal data"*

During this period **10 (ten) practices** are examined and **7 (seven) decisions** are provided. Requests for authorization of the Commissioner for international transfer of personal data has marked new rhythms in their processing due to administrative investigations carried out by the Commissioner's Office ex officio or on basis of complaints, also due to the approval of the new instruction and guideline, which guides and simplifies the manner to be followed by every controller in cases of addressing a request for transfer. The used standard is contemporary and in line with the best international practices.

In cooperation with the Information Center of EU, two opened lectures are organized for the right to information and personal data protection with journalism students of Elbasan and Tirana University.

Training is conducted in the School of Magistrates in the field of personal data protection. Training aimed to make awareness of magistrates on the importance of the protection of personal data during their activity.

Training is conducted with State Policy with spokesman of this directorate on regional level, aiming to sensitize regarding the importance of the protection of personal data and privacy when providing press releases and data disclosure through their publication in the media.

The Commissioner's Office organized on 26 June 2015, in the premises of "Hotel Tirana International", the workshop "Cloud Computing and security measures for personal data protection". This activity was attended by representatives of some institutions as the Authority of Electronic and Postal Communications (AEPC), National Agency of Information Society (NAIS) and by many private companies, which provide Cloud service in our country. The Commissioner's Office acquainted the participants with the guideline on Cloud Computing. In this regard, it invited the attendees that through their experiences contribute widely to further improve of the standards of collection, processing, disclosure and safeguarding data by operators that provide this service in our country in compliance with th e legislation in force and best advanced international practices.

In the premises of the Commissioner's Office, a meeting on 30 September 2015 took place with experts of Council of Europe, Ms. Tea Jaliashvili, Mr. Graham Sutton and Ms. Sylvie Lausy, representatives of the joint project EU/CE – "Suport to the Efficiency of Justice – SEJ". This project is focused in developing our

justice system, where one of the main aspects is the protection of personal data and particularly the anonymization of personal data prior to publication of court rulings in the portal gjykata.gov.al.

The Office of Information and Data Protection Commissioner was present with its stand in the 18th Book Fair "Tirana 2015". This was the second attendance of the Commissioner's Office in this activity, which was conducted on 11-15 November in the premises of Palace of Congresses in Tirana. The presence of Commissioner's Office in this event was a valuable contribution in order to interact directly with the public aiming to foster awareness in acquainting citizens with their constitutional rights: the right to access public information and the right to privacy and personal data protection.

The Office of Information and Data Protection Commissioner conducted a meeting on 24 November 2015 with representatives of EUROJUST, respectively with Ms. Malci Gabrijelcicand Mr. Xavier Tracol. In this meeting were addressed matters regarding the steps for the improvement of legal framework in the field of personal data protection, their compliance with other national acts and with internal acts of Albanian law enforcement agencies. Another case discussed in the meeting was the anonymization process of personal data before the publication of court rulings. The meeting is part of a preparatory process in order to draft a cooperation agreement with EUROJUST.

On 28 January 2016, in the European Personal Data Protection Day, at the premises of National Gallery of Arts in Tirana, the Commissioner's Office organized an awards ceremony for the competition "Protect your Privacy during the navigation on the internet". This kind of activity is considered as one of the best ways to raise awareness and acquaint the youths and children with their rights in order to protect privacy and personal data considering the rapid development of social networks. The organization of competition "Protect your Privacy during the navigation on the internet" with primary schools with works on essay and poetry and in drawing and painting is an initiative of the Commissioner's Office as part of the celebration of 28 January, European Day of Personal Data Protection. In cooperation with Ministry of Education and Sports, this activity was attended by 21 primary schools from 17 cities of the country, pupils of which delivered 500 works in total for the two categories.

The Commissioner's Office conducted with pupils and teachers of 14 high school of Tirana during January – May 2016, the awareness campaign "Privacy and data safety when using social networks by the youth". This activity was organized in cooperation with Education Directorate of Tirana and the respective Directorates of high schools and the staff of the Commissioner's Office informed on various aspects of the safe use of internet and different social networks and on means and ways to avoid the breach of privacy and personal data protection.

The Commissioner's Office in cooperation with the Information Center of EU, organized two meetings with journalism students of Tiarana and Elbasan University. The purpose of these informing acivities was to raise future journalists' awareness on public authorities' transparency, the right to information and personal data protection, while a free and independent media is guaranteed.

The Information and Data Protection Commissioner' Office conducted a 2-day training seminar at the School of Magistrates "Protection of personal data in the judicial system". In this seminar various topics were addressed related to the manner of functioning of the Commissioner's Office; the legitimacy of data processing and data subject rights; the administrative investigation process and the viewpoint of the new Code of Administrative Procedures; personal data protection in the judicial system; the practice of the European Court of Human Rights and personal data; as well as the legislative reform in the field pf data protection in the European Union.

The Commissioner's Office conducted on 15 of April 2016, a meeting with State Police with attendace of spokesman of the Directorate of State Police on regional level. The staff of the Commissioner's Office addressed in this activity issues and concrete cases in the field of privacy protection and the right to information. In this training, special attention was assigned to the balance between public interest on the activity of the structures of State Police and publication os citizens' personal data.

27th edition of Case Handling Workshop

The Office of the Information and Data Protection Commissioner organised in September "27th edition of Case Handling Workshop".
Participating in this activity, being the most important of this format and held for the first time in Albania, were representatives from 18 counterpart Authorities for Personal Data Protection, members of European Conference and three observers delegations. The attendants in the meeting discussed, along the two days of the agenda, and shared the best experiences at the technical level in this field. Part of the program of this meeting were not only the presentations of the work of the counterpart Authorities for Personal Data Protection, but also private controllers assuming their activity in our country, bringing their positive experiences in this field.
Following the organisation of this activity, the Office of the Commissioner prepared the Case Handling Workshop Handbook, as a conclusive document of the activity, due to be published in the official website of the European Commission.

Procedure for certifying Albania as a country ensuring an adequate level of personal data protection

The Office of the Commissioner has instituted the legal procedures for lodging the full file with the European Commission to be enlisted among the countries ensuring an adequate level of personal data protection upon the decision of this organisation. The attainment of this objective facilitates and standardises the sharing of personal data at national level with EU countries.

Involvement in GPEN network

The Albanian authority for the first time made a presentation on its role and its cooperating activity during GPEN meeting, in the context of the 37th International Conference of Privacy and Data Protection Commissioners, held in Amsterdam, inter alia, informing about the relationship with the counterpart Italian authority and signing up the practical cooperation agreement with the latter. This agreement relied on the Resolution on Enforcement Cooperation, approved during the 36th International Conference of Privacy and Data Protection Commissioners held in Mauritius in 2014.

Participation in the International Working Group Data Protection in Telecommunications (Berlin Group - IWGDPT)

The Office of the Commissioner joined the Berlin Group and attended for the first time the 59th IWGDPT Meeting in Oslo, Norway, on 25-26 April 2016.

Observer status at Article 29 WP

Following the application with the Secretariat of Article 29 Working Party, at the Data Protection Unit of the Justice and Consumers Directorate General of European Union, for the accession of the Office of the Commissioner at this organisation in the capacity of the observer, we have been notified by this Secretariat on 27 November about the admission of our Authority as a member in the capacity of the observer.
The acquisition of the observer status by the Office of the Commissioner is an important step towards the European integration of our country and it confirms the observation of the standards of Albanian legislation, drafted in accordance with the EU. To this date, the Commissioner's Office attended the 104th and 105th Plenary Meetings of Article 29 WP.

Participation at the International Conference

The Office of the Commissioner attended the sessions of the 37th international Conference of Privacy and Data Protection Commissioners, under the motto "*Building cooperation Bridges*". The activity was held during 26 – 29 October in Amsterdam of Holland attended by more than 700 officials and international invitees. This was the biggest and most important forum in the field of personal data protection in the

world, where experience is being shared regarding the strengthening the law, enhancing international cooperation and presentation of best practices.
The Office of the Commissioner has, for the first time since its accession, attended this Conference by way of contributing through two presentations in two very important panels. The focus in the panel dedicated to the GPEN global network (Global Privacy Enforcement Network) was on the cooperation among the counterpart institutions, whereby specific attention was assigned to the cooperation agreement with the Italian Authority - Garante per la protezione dei dati personali – and on the joint inspections surrounding, while in the activity on digital education it shared its experience in organising the schools competitions, as a very efficient instrument of awareness with young age groups on the importance of protection of privacy and personal data.

TAIEX

In the context of support provided for institutional activities by the EC Instrument Taiex, the Office of the Commissioner has applied and subsequently conducted a study visit at the counterpart Authority for Data Protection of Czech Republic, with focus on inspections and investigations in the field of data protection and also regarding the functioning of this DPA.

Moreover, the Office of the Commissioner applied in March 2016, for the organization of a workshop on Data Protection in the Media, and was subsequently notified by Taiex that the latter shall finance and organize it. This event anticipates the participation of leading EU authorities' experts and its focus will be the introduction of various media stakeholders in Albania with the new GDPR, best practices of data protection implicating minors in the EU countries, while the aim will be to raise awareness and encourage media stakeholders to comply with the legal framework on privacy and data protection.

Tailor-Made Training (TMT) project

The Commissioner's Office applied for a project with EP – Nuffic, which was approved and will be funded by the latter. This training shall address best practices and experiences on data protection issues, as well as in the field of freedom of information and it is due to take place on 12 – 23 of September in the Netherlands.

ARMENIA / ARMENIE

Major Developments in the Personal Data Protection in Armenia

The major developments in the Republic of Armenia with regard to personal data protection since July 2015 are:

- **Adoption and implementation of a new legal and institutional framework in the field of data protection.**

The new Law on data protection of the Republic of Armenia (the Law), which was adopted by the Armenian Parliament on 18 May 2015, entered into force on July 1, 2015.
The Law reflects the European fundamental data protection principles and standards, mainly, the requirements of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and Directive 95/46/EC of the European parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- **Based on the Armenian law on Personal Data protection new supervisory authority - Personal Data Protection Agency of the Ministry of Justice was established.**

The Agency is operational since 9 October, 20116 when the first Head of the Agency was appointed. In accordance with the law, the Head is nominated for a period of 5 years by the Prime Minister of the Republic of Armenia upon the proposal of the Minister of Justice, on the basis of joint recommendations of at least five non-governmental organisations carrying out law enforcement activities. The candidate for the head of the authorised body nominated by the Minister of Justice of the Republic of Armenia to the Prime Minister of the Republic of Armenia must be from the list of candidacies suggested by non-governmental organisations. The candidate for nomination is presented to the Minister of Justice by common proposal of five NGOs active in the Human rights protection.
The Agency's functions are:
- checks the compliance of the personal data processing (PDP) with the requirments of the Law;
- orders blocking, suspending, or terminating of PDP violating the Law requirments, rectification, modification, or destruction of personal data;
- prohibits completely or partially the PDP as a result of notification,
- ensures the protection of rights of data subject;
- recognises electronic systems of legal persons as having an adequate level of protection;
- initiate administrative proceedings and applies administrative sanctions in case of the Law requirments violation;
-examines application of natural persons regardinf PDP and delivers decisions.

- **Completed tasks**

As of May 1, 2016 since its operation in October, 2015, the Agency:
- provided consulatations to 251 legal and natural persons, including 53 state institutions, 175 legal persons, 16 citizens, 4 journalists and 3 NGOs;
- delivered 7 decisions - 2 advisory decisions on protection of personal data of children and direct marketing issues, 4 on the basis of administrative proceedings on various aspects of data protection law violations and 1 official position on biometric data;
- conducted trainings for 311 controllers - out of which 51 from state institutions and 260 from legal private bodies.

- **International cooperation** - In 2016 the Agency became a member of:

- Global Privacy Enforcement Network (GPEN);
- Central Eastern European Data Protection Authorities (CEEDPA);
- International Working Group on Data Protection in Telecommunications (Berlin Privacy Group);
- Personal Data Protection Agency was accredited as member of the Conference of European Data Protection Authorities with the status of European national Data Protection Authority.

AUSTRIA / AUTRICHE

Major developments in the data protection field in Austria 2015/2016

- the annual report of the Austrian Data Protection Authority (Annual Report 2015) is available in German at http://www.dsb.gv.at/DocView.axd?CobId=62793
- In its judgment of 8 October 2015, G 264/2015, the Austrian Constitutional Court declared Section 28 para 2 of the Austrian Data Protection Act 2000 (right to object without giving reasons) invalid; the judgment is available in German at http://www.ris.bka.gv.at/Vfgh/.
- legislation/legislative procedure:
    - the Austrian Parliament adopted the Police State Security Act (*Polizeiliches Staatsschutzgesetz*) which gives the intelligence branch of the police broader competences; the supervisory role of the Austrian DPA remains untouched
    - the Ministry of Justice plans to introduce surveillance measures concerning incoming and outgoing messages that are transmitted via computer systems; the Austrian DPA issued an opinion on that matter which is available at https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06768/index.shtml.

BELGIUM / BELGIQUE

Développements majeurs intervenus dans le domaine de la protection des données en 2015 : BELGIQUE

Principales activités de la Commission belge de la protection de la vie privée (BE)

L'année 2015 a été marquée par les démarches entreprises par la Commission belge de la protection de la vie privée (CPVP) sur les pratiques de Facebook. Ce qui avait commencé par un simple examen des nouvelles conditions générales du réseau social au début de l'année 2015 s'est « terminé » par une condamnation en référé de ce géant du Net.

- L'année où Facebook s'est retrouvée dans la ligne de mire

L'analyse des conditions d'utilisation de Facebook a donné lieu début 2015 à son audition ainsi qu'à une recommandation (n° 04/2015) adressée à Facebook elle-même, aux exploitants de sites Internet et aux internautes à propos de l'utilisation de 'plug-ins' sociaux. En mai 2015, le groupe Facebook a été mis en demeure pour violation de la Loi vie privée belge (Loi du 8 décembre 1992) et de l'article 129 de la loi belge relative aux communications électroniques. Facebook a été sommée de mettre fin à ces violations, mais elle n'y a pas donné suite. Il s'en est suivi une citation en référé et un jugement du Tribunal de Première instance de Bruxelles siégeant en référé, le 9 novembre. Ce jugement condamne Facebook Inc., Facebook Ireland Limited et la SPRL Facebook Belgium à cesser l'enregistrement, via des cookies et des plug-ins sociaux, des habitudes de navigation des internautes belges ne disposant pas d'un compte Facebook (les non utilisateurs). Une astreinte de 250.000 EUR a été infligée par jour de non-respect. À la suite de ce jugement, Facebook a décidé de bloquer l'accès à ses pages "publiques" aux Belges qui ne sont pas membres du réseau social. Appel a également été interjeté par Facebook contre cette première décision en référé. La procédure au fond poursuit quant à elle également son cours.

Les principaux enseignements du jugement en référé :

- Compétence de la CPVP et droit belge applicable : Le tribunal affirme que le droit belge en matière de protection des données est d'application et que les tribunaux belges sont compétents. Facebook avait argumenté qu'elle ne devait respecter que le droit irlandais en matière de protection des données et que seuls les tribunaux irlandais étaient compétents. Le tribunal n'a toutefois pas partagé cette ligne de défense et s'est appuyé sur l'arrêt de la Cour de Justice de l'Union européenne dans l'affaire C-131/12 Google Spain c. Agencia espanola de Proteccion de Datos et M. Costeja selon lequel le droit national en matière de protection des données d'un Etat membre de l'Union s'applique si les activités d'un établissement local de cet Etat membre sont indissociablement liées aux activités du responsable de traitement. Le tribunal affirme que c'est le cas en l'espèce dès lors qu'en Belgique, la société Facebook SPRL Belgium existe et que cette société locale réalise un travail de lobby pour le groupe Facebook et participe au marketing et à la vente d'espaces publicitaires du service Facebook.

- Violation de la législation belge en matière de protection des données

Le tribunal estime que la collecte par Facebook de données sur les habitudes de navigation de millions d'internautes en Belgique ayant fait le choix de ne pas être membres du réseau social constitue une violation manifeste du droit belge en matière de protection des données. Le tribunal souligne entre autres points que Facebook ne peut invoquer aucune justification légale pour le traitement via des cookies et des plugs-in sociaux, de données personnelles de personnes non titulaires de comptes Facebook car :

o Facebook n'a pas obtenu de consentement à cette fin

o Facebook ne peut invoquer de contrat avec des personnes qui ne disposent pas de compte Facebook

o Facebook ne peut se fonder sur une obligation légale à laquelle elle serait tenue

o Le droit fondamental au respect de la protection de la vie privée des personnes ayant fait le choix de ne pas disposer de compte Facebook prévaut sur les intérêts de sécurité invoqués par Facebook. Quant à cet argument « sécurité » invoqué par Facebook, le tribunal juge peu crédible que pour la sécurité des services Facebook, il soit nécessaire de consulter les cookies « datr » chaque fois que qu'un plug-in social est chargé sur un site Internet.

 Cookies, drones et mesures anti-terroristes

La Commission belge de la protection de la vie privée s'est également exprimée sur une série de thèmes d'actualité importants, parmi lesquels l'usage croissant de cookies et de drones ainsi que sur des projets de mesures anti-terroristes du gouvernement fédéral, notamment à la suite des attentats de Paris et Bruxelles.

- Cookies :afin de répondre aux multiples questions qui se posent quant à l'utilisation des cookies, la CPVP a formulé une série de recommandations. Celles-ci ont pour but d'informer les juristes, techniciens, annonceurs et développeurs de sites Internet sur les pratiques de marketing direct et sur l'importance de la communication d'informations.

- Drones : Le projet d'arrêté royal relatif à l'utilisation de drones a reçu un avis positif car il tient suffisamment compte de la législation en matière de protection de la vie privée. La CPVP relève que le projet de texte ne laisse aucun doute sur le fait que la législation en matière de protection des données s'applique intégralement aux drones lorsque des données personnelles sont traitées avec l'intervention d'un drone. Le projet d'arrêté royal s'applique à tous les drones, même aux aéronefs télépilotés qui, dans la pratique, suscitent plus de questions et d'interrogations (usage récréatif).

- Mesures de lutte contre le terrorisme : La Commission vie privée s'est par contre montrée plus réticente dans ses avis sur le traitement des données de passagers (avis 55/2015), sur un projet de création d'une banque de données commune pour les "foreign terrorist fighters" (avis 57/2015) et sur la suppression de l'anonymat pour les utilisateurs de cartes prépayées (avis 54/2015).

 Sensibilisation et guidance : droit à l'image et vie privée sur le lieu de travail

Par ailleurs, la Commission vie privée a vu se confirmer la tendance à la hausse de ses dossiers de décisions individuelles.

2015 a été pour la plate-forme des jeunes "Je décide" l'année du droit à l'image. Un dépliant informatif et un kit pédagogique à l'attention des enseignants ont été élaborés afin d'apprendre aux jeunes à adopter une attitude plus consciente et plus respectueuse de la vie privée lors de l'utilisation d'images. http://www.jedecide.be et http://www.ikbeslis.be

Enfin, compte tenu du nombre croissant de questions sur des aspects spécifiques en relation avec la vie privée sur le lieu de travail, la CPVP a publié en 2015 un dossier consacré à cette thématique sur son site Internet. Ce dossier entend proposer des réponses aux questions que se posent tant les employés que les employeurs sur la manière de traiter des données à caractère personnel sur le lieu de travail de manière correcte et en respectant la vie privée. Il aborde entre autres problématiques, celle de la géolocalisation dans les véhicules de société, de la surveillance par caméras et de la surveillance électronique via l'e-mail et Internet.

L'ensemble des documents, avis, lignes directrices et autres information mentionnées ci-dessus sont disponibles dans leur intégralité, en français et néerlandais, sur le site de la Commission belge de la protection de la vie privée (http://www.privacycommission.be) ainsi que dans son rapport annuel 2015 disponible sur ce même site.

BOSNIA AND HERZEGOVINA / BOSNIE ET HERZEGOVINE

Subject: **The most important activities in the field of personal data protection in Bosnia and Herzegovina for the period May 2015 - May 2016**

Personal Data Protection Agency in Bosnia and Herzegovina was established by the Law on Protection of Personal Data ("Official Gazette of BiH", No. 49/06) and it has started its work in June 2008. Law on Amendments to the Law on the Protection of Personal Data ("Official Gazette of Bosnia and Herzegovina" 76/11) was adopted by Parliamentary Assembly of Bosnia and Herzegovina in 2011. By the Ordinance on internal organization and job classification, 45 working places were systematized in the Agency. The Agency currently employs 26 officers.

Normative activity

During the reporting period, the Agency has prepared a proposal for Amendments to the Election Law of Bosnia and Herzegovina and delivered it, via the Central Election Commission of Bosnia and Herzegovina, to Intersectoral Working Group for amendments to the Election Law of Bosnia and Herzegovina. During the reporting period 12 verdicts of the Court of BiH were issued in favour of the Agency and 19 statements of defence were delivered.

According to the Agency's activities that were implemented during the reporting period, the state of personal data protection in our country could be described as satisfactory. Statistical indicators in all segments, except inspections and registration of controllers, moved upward. This is evidenced by a significant increase of the number of submitted complaints of citizens indicating increasing of awareness of the importance of personal data protection.

In the reporting period 107 decisions on the objections were made, mostly against public authorities, as well as against other controllers such as banks, micro-credit organizations and other economic entities and natural persons, and 168 activities were performed in the proceedings on the complaints. The reasons why the complaints were submitted are, inter alia, the special treatment working years, processing of data on health status and treatment of biometric data, data delivery to a third party, video surveillance, copying and retention of personal documents, direct marketing, publishing of the information on the website and so on.

A large number of requests for an opinion (sent from public and private sectors) witnessed about increasing of awareness of all entities on the protection of personal data. 252 such requests and 31 responses were sent during the reporting period (12 of these opinions were about personal data transfer abroad).

It is important to mention that in the past period the Agency received a large number of requests for opinion about concrete demands for access to the information in contest procedure which are, on the basis of the Law on Free Access to Information, delivered to public authorities. In this regard, the Agency published its formal attitude and opinion on this subject on its official webpage, http://www.azlp.gov.ba, in the opinion – "Access to the documents of the candidates selected in public contest". In that way we enabled, for a huge number of persons who are interested in this subject, to be informed, with no particular verbal or written addressing to the Agency, about the legal basis and right to access to documents of the candidates in contest procedure, as well as about the manner and scope of personal data that are delivered or disclosed.

In performing its regular surveillance activities in the reporting period, the Agency performed 96 inspections (1 audit, 55 regular and 40 extraordinary supervisions), prepared 30 Decisions ordered by administrative measures, 30 ex officio Decisions, registered 97 new controllers and entered 99 records of personal data.

The Agency has started issuance of misdemeanor warrant in 2011 and in the reporting period has issued 8 misdemeanor warrants.
The Agency continued with training activities for controllers in the public sector across the whole country in order to increase the capacity of personal data protection within the public administration and the police. During the reporting period 22 trainings were held

Cooperation with media

The Agency regularly informs the media about its competencies and activities, promotes the work of the Agency and informs the public regarding the processing and protection of personal data. The Agency commonly responded to all media inquiries and reported on time through all available means of public information and by publishing opinions and decisions on the official website of the Agency, as well as through the Help desk.
In connection with the above, the press conference was held on the occasion of the European Data Protection Day, 28 January 2016. At various queries of print and electronic media 10 written responses and 4 statements were given and there were 7 appearances in the media, 654 inquiries of citizens were replied through the Help desk of the Agency. Website of the Agency is regularly updated by necessary contents which shows commitment to transparent work of the Agency. In the reporting period there were 13 158 recorded visits to the Web site of the Agency. In the media and in the Internet there were 138 published articles, concerning the activities of the Agency and the protection of personal data.
Bosnia and Herzegovina hosted 18th Conference of Central and Eastern European Data Protection Authorities – CEEDPA, which was held on 11th and 12th May, 2016 in Sarajevo and which was organized by Personal Data Protection Agency of BiH. There were 52 participants from 16 member states and Council of Europe on 18th CEEDPA Conference.
By adoption of New Member Declaration, Armenian Personal Data Protection Agency became the 20th CEEDPA member.
The host of the next 19th CEEDPA is Georgia.

CROATIA / CROATIE

Major developments in the data protection field - Croatia

The Consultative Committee of the convention for the protection of individuals with regard to automatic processing of personal data (T-PD), in view of the forthcoming 33rd Plenary meeting (29 June – 1 July 2016), has invited the members and observers to send in comments regarding the major developments in the data protection field since the last Plenary meeting held in July 2015. The contribution of Croatian Personal Data Protection Agency to this request is as fallows:

As a part of the Croatian request for admission to the Schengen area, evaluation of the implementation of all areas of the Schengen *acquis* was conducted. Among other things, the Agency was actively involved in answering a standard questionnaire submitted by the European Commission, which includes answers to the questions on the application of all relevant legislation and best practice in the Member State, and in particular the application of organizational and technical resources that are available in implementation of the Schengen *acquis*. Also, *in situ* evaluation was conducted in the field of data protection and the Schengen Information System, in order to estimate the competence of the Croatian supervisory body (the Personal Data Protection Agency) in the implementation of activities on personal data protection in the Schengen Information System and Visa Information System.

In cooperation with the Croatian Employers' Association, the Agency has initiated and conducted national series of training on the legality of the processing of personal data intended for the controllers (economic entities in the Republic of Croatia) and officials for the protection of personal data. The purpose of the measures conducted was to promote the continuous training and new skills to the employees, especially in the use of new information technologies in personal data processing, with emphasis on clearer understanding of the data protection legislation and therefore more effective implementation of the Personal Data Protection Act.

CYPRUS / CHIPRE

Major Developments in the data protection field (CYPRUS)

1. Since the last T-PD Plenary Meeting we had the appointment of the new Commissioner for Personal Data Protection Ms Irene Loizidou Nicolaidou as of September 28th 2015.

2. In the framework of the Multilateral Competent Authority Agreement on the Automatic Exchange of Financial Account Information 27/01/2016, the Decree of the Cyprus Tax Department, has been issued in December 2015.

3. Following the Decree of the Commissioner for Electronic Communications and Postal Services with regard to Data Breach Notification (May 2015) our Office prepared a draft Memorandum of Understanding (April 2016) between the two Commissioners which is aiming at providing the procedure in line with the joint competence of the two Offices.

4. The Ministry of Justice and Public Order prepared a draft bill regulating citizen's right to public documents (FOI Bill). According to the draft bill the Commissioner will undertake new competences.

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

Major developments in the data protection field in the Czech Republic since June 2015

1. The Office for Personal Data Protection of the Czech Republic (hereinafter “the Office”) has been a kind of guarantor that the drafts for plans and legislation included an assessment of the impact on personal data protection and privacy in accordance with the legislative rules (DPIA). Aside from specific proposals and comments, the Office also intervened with a general warning in cases where the responsible ministries – the submitters of bills – had overlooked issues of personal data protection and privacy and instead of an expert assessment had included a political proclamation of the type, "*The proposed legislation fully respects the interest of personal data protection and does not in any way interfere with this interest*." In such cases the Office most frequently pointed out the absence of an evaluation of newly introduced information technologies and automated data processing, the misunderstanding of the mechanisms of data management and the inability to identify changes and potential risks in the processing and securing of personal data. The Office's basic general comment is often a simple warning that if personal data are processed, particularly on the basis of law, it always has an impact on the protection of privacy and personal data. The goal of the DPIA is not just to make an assessment of whether this impact is positive, neutral or negative, but rather the assessment of the method and risks of the proposed and existing processing of personal data. In the comment proceedings it is asked that the proposer clearly state whether the legislative proposal establishes new processing of personal data; if so, with what basic parameters, including but not limited to: specific purpose, category of personal data processed, the public or private law nature of the processing, part thereof, or output from processing, and the retention period for personal data.

2. The Office had crucial objections to the drafting and method of approval of an amendment that added a legal basis for information database on the financial standing and credit history of consumers to Act No. 634/1992 Coll., on Consumer Protection. This was a complicated piece of legislation that was not prepared in the standard consulting procedure, i.e. on the basis of a government draft prepared by the competent ministry. The treatment of the aforementioned database is in essence a special law that has merely been formally inserted into Act No. 634/1992 Coll. As the legal treatment of the database was inserted into the act by a mere amendment proposal, the government did not comment on it and the bill did not receive the attention that such a fundamental matter deserves. Around the same time the government approved a draft Act No. 145/2010 Coll., on Consumer Credit, and the Chamber of Deputies of the Parliament of the Czech Republic discussed it as a separate item – that would have been a much more appropriate platform for regulating a consumer credit register. The Office pointed out a number of practical and legislative technical shortcomings in the draft, as the Parliament-initiated bill did not address fundamental legal obligations in the processing of data, from the legal reason (purpose) and principle of proportionality (substantiality) of processing personal data to the obligation to retain personal data only for the necessary period. The Office requested that the overall objective – protecting the legitimate interests of providers – would be the subject of public consultation with the stakeholders.

3. The Municipal Court in Prague stated that the service provider is not obliged to monitor content of transmitted or saved information, nor to actively retrieve facts and circumstances demonstrating the unlawful content of information and is thus not liable for the content of information inserted by users. This ceases to apply however from the moment that the service provider learns of the unlawful nature of the content of such information. Recognised as such a moment was the receipt of a letter from the Police of the Czech Republic asking for information on the poster of a specified post due to an investigation pursuant to Section 158 (1) of Act No. 141/1961 Coll., the Criminal Code. Such a communication may not be left unnoticed and the service provider should address the post on the basis of such. Thus, if a certain entity organises an internet discussion on its website, it must invest the effort and resources to cultivate the chat and continually remove expressions that could affect the reputation of third parties. In no case this responsibility might be avoided by saying that the author is not the organiser and contributors cannot be restricted in any way because the "internet is free".

DANEMARK / DENMARK

General Information

In August 2016 Ms. Cristina A. Gulisano was appointed director of The Danish Data Protection Agency. Ms Cristina A. Gulisano has previously worked for The Danish Data Protection Agency and The Ministry of Justice.

Information on case-law

CSC hacker attack

In 2015 The Danish DPA finalized its processing of the case concerning unauthorized access to personal data in systems for which the Danish National Police is data controller.

The case started in connection with the police's investigation of a hacker attack on information systems that were operated at CSC on behalf of Danish authorities where it was revealed that there inter alia was an unauthorized access to the Danish National Police's information systems on the hacked mainframe, including data from the Schengen Information System.

After being made aware of the hacker attack in May 2013 the Danish DPA initiated an investigation of the case.

The Danish DPA concluded that the Danish National Police had failed to comply with the requirements on security in the Danish Act on Processing of Personal Data and in the Schengen Convention. Furthermore, the Danish DPA criticized the lack of notification from the Danish National Police to the affected group of persons about the unauthorized access to personal data.

Automatic Number Plate Recognition

During 2015 the Danish DPA several times gave its opinion concerning the Danish police plans on implementing an automatic number plate recognition system. The system is able to automatically identify number plates on cars driving by and can be used by the police in their investigation but also for other purposes such as analyzes.

The Danish DPA expressed its concerns about the amount of data collected by the system and the time span the police would keep the data before deleting it. For these reasons the Danish DPA stated that the processing of the personal data from the system ought – at the least – to be in an Executive Order.

Other important information

Greenland

The Danish Act on Processing of Personal Data does not extend to Greenland however it may by Royal Decree be given effect for the processing of data by the constitutional authorities subject to any deviations following the special conditions in Greenland. The Government of Greenland has now expressed its wish that the Danish Act on Processing of Personal Data is implemented in Greenland.

The Danish DPA is assisting the Danish Ministry of Justice and the Government of Greenland in this work.

Binding Corporate Rules (BCR)

The Danish DPA used considerable resources in the processing of 6 BCR's where the Danish DPA was "lead DPA".

FINLAND / FINLANDE

The major developments in the data protection field in Finland in 2015

Summary of activities and news

The Data Protection Ombudsman continued active participation in the work of the Human Rights Delegation, based on the Paris Convention. The focus areas of this work include the inclusion of education on basic and human rights, including data protection, in school curricula, and action against hate speech in collaboration with other authorities responsible for the supervision of basic and human rights in Finland.

Together with the partners, he contributed to the launch of training programmes directed at Data Protection Officers. He also provided training on the EU's Data Protection Regulation.

In line with the strategy, the Data Protection Ombudsman completed a study on data management in the public administration, together with the National Archives Service. Several serious deficiencies were detected. Studies and measures to counter such deficiencies were also executed in the health care and pharmacies sector. In addition, in cooperation with the data protection authorities of Norway, Denmark and Iceland, he conducted an inter-Nordic inspection whereby the competent authority of each country inspected the legality of the processing of consumers' personal data. The project benefited the development of international cooperation, while supporting preparation for new duties related to the European Union's reformed Data Protection Regulation. For the purposes of the transition to reformed Regulation, he collaborated on preparing plans for projects to be implemented in various Nordic countries, and agreed on the checkpoint for their implementation.

Codes of practice were confirmed e.g. for universities and operators in the affiliate industry. Furthermore, the office of Data Protection Ombudsman provided guidance on issues such as the biobank industry.

The increase in the number of data protection offences continued. The office of the Data Protection Ombudsman issued a total of 227 statements to public prosecutors and courts of law. During the year under review, the amendments to the Criminal Code of Finland regarding cybercrime entered into force, criminalising so-called identity theft.

It was a pleasure to witness the increasingly common use of the data balance sheet, developed by the office of the Data Protection Ombudsman. The data balance sheet is a method of implementing the accountability principle. Its use is linked to the digitalisation process implemented in Finland, based on the Government Programme. The Data Protection Ombudsman contributed to the preparation of the National Information Security Strategy and guidance of information security work in municipalities.

The Data Protection Ombudsman published six Safe Harbor notices. He also began the preparation of implementation measures required in law enforcement. There is no longer publishing a printed version of the Tietosuoja magazine. Instead, the Data Protection Ombudsman is increasingly focusing the efforts on digital communications. The internal quality management efforts continued.

Information on case-law

The well-known “Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland (no. 931/13)”, previously heard at the European Court of Justice, was also heard by the European Court of Human Rights (ECHR). The court decided that no violation of freedom of speech had taken place, but processing of the case will continue in the ECHR Grand Chamber.

The Data Protection Ombudsman lodged an appeal with the Supreme Administrative Court regarding an appellate court's decision in a case concerning the processing of personal data by a religious community and its members. The issue to be decided on concerns the controller.

In its decision KKO 2015:41, the Supreme Court applied the Act on the Protection of Privacy in Working Life, stating that the job applicant had faced discrimination when e.g. personal data of a sensitive nature had been collected without reason.

The Data Protection Board's decisions, with regard to the justified interests of the controller, have concerned issues such as the use of WiFi connection points' MAC addresses etc. for the purposes of constructing a positioning service infrastructure, and the provision and development of services, the provision of map services, and an internet-based service related to city archive material containing personal data. The cases also involved an evaluation of the necessary security guarantees.

Other important information

During the year under review, an increasing number of problems were related to the transnational provision of services. Electronic direct marketing that originated abroad but violated Finnish law, supranational scientific research projects, various overlay services and, in particular, the services of the financial sector confirm that there is a need for the harmonisation of data protection regulations. Technological advances and development in the use of technology posed further challenges for us, including the national service channel, digital influence, ‘digital sharing economy’ and positioning data (‘Big Brother Airport’).

Mainly due to the Finnish Constitution, we have a remarkable number of special acts governing personal data protection and privacy. The reformed EU Data Protection Regulation will therefore require the considerable reassessment and updating of legislation in this country. At the same time, however, deregulation efforts are being agreed on in the Government Programme of the current Cabinet. Due to these two issues, and for other reasons, the Data Protection Ombudsman launched a special project in 2015 to manage the transition to the new Regulation. The project plan was partially prepared in cooperation with our colleagues in the Nordic countries.

Due to the identification of international threat scenarios in particular, preparations were made for the initiation of data network traffic supervision in Finland. At the same time, the agency of the Data Protection Ombudsman contributed to the preparation of the National Information Security Strategy and instructions for data security work in municipalities. This gave the ECJ judgment (C362/14, Schrems) a special emphasis in this country.

Data protection of children and young people was a key focus area in the operations of the Data Protection Ombudsman. It contributed to integrating data protection in projects preventing the social exclusion of juveniles, student care services, national competence and learning systems, and the teaching of media skills.

GEORGIA / GEORGIE

Major Developments in the Data Protection Field

July 2015 – June 2016

Georgia

LEGISLATIVE AMENDMENTS

Taking into account current data protection reform on the Council of Europe and European Union level the Office of the Personal Data Protection Inspector of Georgia prepared draft legislative amendments to the Law of Georgia on Personal Data Protection and 9 other related legal acts. The legislative proposal enhances the scope of application of the Law of Georgia on Personal Data Protection, it introduces new regulations on data processing for historical, statistical and research purposes and on audio-monitoring; improves existing video-monitoring and direct marketing regulations, amended rules on direct marketing establish an electronic registry of direct marketing providers in order to ensure accessible online opt-out mechanism; furthermore, for the protection of data subjects' rights and for increasing effectiveness of the Personal Data Protection Inspector, draft provides amended rules for examination of the complaints and conducting inspections. Last but not least, fines for breaching data processing rules are increased.

Inspector's Office organized several roundtables and discussed the draft with representatives of ministries and other public bodies, private, non-governmental and international organizations, as well as all fractions of the Parliament of Georgia. With the invaluable assistance of the CoE, the draft was reviewed by the CoE legal experts. Together with the expert review, the Council of Europe and the Inspector's Office organized wide discussion of the draft in April 2016.

ACTIVITIES OF THE INSPECTOR'S OFFICE AND FIGURES

As a result of the activities of the Inspector's Office video and audio monitoring processes by different organizations came in line with existing legislation, access to databases by staff of Ministry of Internal Affairs of Georgia, Public Service Development Agency and other big data holder public institutions was improved, the standards of data processing of juveniles being in conflict with law were improved and relevant internal regulations were adopted by the Ministry of Corrections of Georgia. Accessible opt-out mechanism from direct marketing has been also introduced by number of organizations. The Office of the Personal Data Protection Inspector of Georgia actively worked with the judiciary and civil society organizations on the issue of access to court judgements and to strike right balance between access to information and privacy.

In 2015 the number of complaints discussed by the Inspector's Office increased 6 times and consultations provided to different public and private organizations as well as individuals tripled. Number of inspections has also increased and amounted to 54 in total, involving 38 private and 16 public bodies; As for the numbers for January-May 2016, the Inspector's Office has already conducted 42 inspections, discussed 71 complaints and provided 1115 consultations.

Staff number has also increased up to 43 and the budget of the Office - to 2 100 000 GEL.

Numerous activities were carried out in terms of awareness raising. Consultative and informational meetings were organized in capital and regions for different target audiences. Different types of informational materials, sector specific guidelines/recommendations and Public Service Announcements were prepared during 2015-2016. Photo, video and poster competition was announced and conducted successfully.

The Inspector's Office delivered 65 trainings and public lectures involving 1600 participants in 2015. During January-May of 2016 22 trainings were provided to 757 participants.

On January 28, the Inspector's Office organized media campaign to underline importance of data protection, rights of data subjects and obligations of data controllers. Furthermore, to commemorate International Data Protection Day the Inspector hosted reception where keynote speakers Prime Minister of Georgia and the Chairman of the Parliament of Georgia addressed representatives of diplomatic corps, international organizations, civil society, business, academia, public sector and media.

LAW-ENFORCEMENT OVERSIGHT

In order to effectively exercise external control over the data processing for police and crime prevention/investigation purposes, the Law Enforcement Oversight Unit was established at the Inspector's Office. In 2015, Law Enforcement Bodies Oversight Unit conducted 20 inspections. With the involvement of the Inspector's Office, illegal practice of gaining Meta data from communication companies and video recordings from private companies by the law enforcement bodies has been eradicated. Furthermore, the Inspector did not authorize interception in the framework of the two-stage electronic monitoring system in 45 cases.

In April 2016 the Constitutional Court of Georgia adopted a decision by which the Court assessed possibility of the State Security Service of Georgia to access real time data for the telephone tapping disproportionate to the legitimate aims. It also considered unconstitutional the right of investigative body to copy and retain Meta data for 2 years. As a result, the Court requested to introduce relevant amendments into the legislation and to develop proper institutional and technical systems before 31st of March 2017. The Inspector's Office will be involved in law making process.

INTERNATIONAL RELATIONS

In October 2015, the Office joined International Conference of Data Protection and Privacy Commissioners (ICDPPC) and Global Privacy Enforcement Network (GPEN), followed by becoming a member of International Working Group on Data Protection in Telecommunications (Berlin Group) in March 2016.

The Office continues to establish close cooperation with Data Protection Authorities of other countries. In August 2015 Memorandum of Cooperation with the DPA of Poland was signed.

The Inspector's Office is actively involved in the approximation process of Georgia with the EU. The Visa Liberalization Action Plan benchmarks related to data protection were deemed to be successfully met by the European Commission in May and December 2015. The Office continues to work in order to implement Association Agreement with the EU.

GERMANY / ALLEMAGNE

Berlin, 23 June 2016

Annual Report of the German Federal Government

to the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) within the Council of Europe

on important developments in data protection law in the Federal Republic of Germany from July 2015 to June 2016

1. Revising German data protection law in line with the EU's General Data Protection Regulation and implementing the EU Data Protection Directive for the police and criminal justice sector

a) As soon as the trilogue on the General Data Protection Regulation was concluded in late 2015, Germany began working to revise its data protection law in line with the new regulation.

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4 May 2016, pp. 1–88) entered into force on 25 May 2016. Starting 25 May 2018, it will be directly applicable law in all member states of the European Union.

The member states thus have two years to amend their national data protection law to comply with the European requirements.

Amendments will be needed because the General Data Protection Regulation contains specific regulatory tasks for various areas. It also gives national lawmakers room to develop data protection law further in certain areas.

In Germany, federal and state law will have to be amended. The Federal Data Protection Act will be affected first of all, but the data protection legislation of the federal states and all sector-specific data protection law at federal and state level will have to be reviewed for its compliance with the General Data Protection Regulation and amended as needed. In view of the member states' responsibility for their intelligence services, data processing by these services will eventually have to be regulated due to the planned changes in general data protection law and the regulatory gaps that will result in some cases. The extent of the legislative amendments needed will require a step-by-step approach. Until the General Data Protection Regulation goes into effect on 25 May 2018, the amending legislation will concentrate in particular on the European requirements to be implemented with priority. This includes above all carrying out the regulatory tasks set by the General Data Protection Regulation, such as the status of independent data protection supervisory authorities in Germany, designating the German representation on the European Data Protection Board and ensuring appropriate guarantees for the lawful exercise of supervisory powers, including relevant legal redress, as well as the use of optionality clauses to take public interests into account.

b) Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision

2008/977/JHA entered into force on 5 May 2016. The member states have two years to implement the Directive. The Federal Government is already engaged in concrete planning for implementing the Directive in the relevant areas of law.

2. Second Act Amending the Federal Data Protection Act (BDSG) – Reinforcing the independence of data protection supervision at federal level by establishing a supreme federal authority

The Federal Government made this amendment to the BDSG in response to requirements of the European Court of Justice. Particularly in its judgments of 9 March 2010 (Case C-518/07) and of 16 October 2012 (Case C-614/10) regarding Article 28 (1)(2) of Directive 95/46/EC, the ECJ formulated more specific requirements for the independence of the authorities responsible for data protection. The new Act meets these requirements and strengthens data protection supervision at federal level.

Effective 1 January 2016, the Federal Commissioner for Data Protection and Freedom of Information acquired the legal status of a supreme federal authority with an autonomous, independent structure. It is located in Bonn. The Federal Commissioner is subject only to parliamentary and court supervision. The Federal Government no longer has legal supervision and the Federal Ministry of the Interior is no longer responsible for its administrative supervision. The Federal Commissioner is no longer organizationally linked to the Federal Ministry of the Interior. The Federal Commissioner is elected by the German Bundestag and takes an oath of office administered by the Federal President. Existing provisions on additional matters such as representation, continued performance of duties, use of gifts, permission of statements and provision of reports were replaced with new provisions that comply with EU law.

3. Implementation of the EU PNR Directive

Directive (EU) 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime was published in the EU's Official Journal on 4 May 2016 and is to be implemented by 25 May 2018. The Federal Government is now working intensively on its legal and technical implementation in German law, in particular with regard to setting up a German Passenger Information Unit (PIU).

4. Judgment of the Federal Constitutional Court of 20 April 2016 on the preventive powers of the Federal Criminal Police Office (1 BvR 966/09 et al.)

The Federal Constitutional Court agreed in part with complaints that the investigative powers of the Federal Criminal Police Office (BKA) for counter-terrorism purposes were unconstitutional. In particular, the court found that data protection law aspects of undercover investigative measures pursuant to the Act on the Federal Criminal Police Office (BKA-Gesetz) must be revised with regard to protection of the core area of private life, to court orders, transparency provisions, legal redress and independent oversight.

The decision develops new distinctions concerning the conditions for using data in a way which goes beyond the original purpose (the criterion "hypothetical re-gathering of data"). In addition, some of the provisions of the Act concerning the transfer of data to domestic and foreign security authorities must be amended in line with the new criteria of the "hypothetical re-gathering of data".

The Federal Government has until mid-2018 to make the necessary legislative amendments.

ITALY / ITALIE

Major developments in the data protection field

Data Protection Law

In the course of 2015 there were no amendments/additions to the current Data Protection Law (Legislative Decree no. 196 of 30 June 2003, "Data Protection Code" available at: http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf).

Main activities of the Data Protection Authority

Opinions - SPID (Public System for Digital Identity Management) and reuse of public sector information - FATCA

The Italian DPA "Garante" issued several opinions to the Italian Government in order to ensure the compliance of new regulations with the data protection principles.

In particular, two opinions were rendered by the DPA (June 2015) to AGID [Italy's Agency for Digitalisation] – namely, a draft regulation with implementing arrangements for the SPID (the public system managing the digital identities of citizens and undertakings) and a draft regulation containing the relevant technical requirements. The drafts were found to be compliant with most of the indications given by the DPA as part of an ad-hoc technical working group; however, the DPA requested additional specifications to be made in order to better protect data subjects. In particular, the DPA highlighted the importance of enhanced security standards for digital identities in the light of the possible consequences resulting from the theft, misuse or alteration of a data subject's identity – via phishing, malware, remote control software agents, or digital counterfeiting of online websites and services. Accordingly, the DPA called for implementing awareness-raising policies along with the adoption of more effective remedial measures. The DPA pointed out some criticalities in the architecture of the SPID such as to give rise to single points of failure that might undermine overall functioning; it also emphasized that the storage periods of information relating to users' identity profiles should be regulated thoroughly.

A favourable opinion on a draft legislative decree transposing Directive 2013/37/EU of 26 June 2013 on the reuse of public sector information was delivered in April 2015. The draft decree had taken on board the indications provided by the DPA as for the reuse of any document in which intellectual property rights are owned by libraries, museums and archives; the limitations placed on accessing documents that contain non-publicly available personal information; and the use of open licences as available online.

Regarding the automatic mandatory exchanges of tax-related information and pursuant to two opinions given by the DPA in July on the FATCA Agreement – which is intended to improve international compliance in taxation matters – in December, the Garante gave a favourable opinion on a decree by the Ministry of Economy and Finance that set forth the technical rules to collect, transmit and notify the Revenue Agency of any information on non-nationals in accordance with applicable international agreements.

Electronic Health Dossier

New Guidelines on the electronic health dossier were adopted by the DPA in July 2015 to lay down a unified reference framework when processing data in this sector as well as to afford enhanced safeguards and top-level security standards to patients. The dossier is a file set up at a given health care body (hospital, nursing home, etc.) containing information on a patient's health and clinical history in order to ensure better, more targeted treatment. As such, it differs from the electronic health record where the whole clinical history concerning an individual is pooled from several health care providers. The Guidelines clarify, in particular, that patients must be enabled to take free, informed decisions on whether a dossier should be set up or not; failing the patient's consent, a physician may only rely on the information disclosed by the patient on the occasion of the current and/or of a previous treatment/visit by/to that physician. An additional, specific consent declaration will be necessary to enter highly sensitive information in a dossier - such as info on HIV-related infections, abortions, rape or paedophilia cases. Patients have the right to view the access logs relating to their health dossiers while certain health data or documents patients do not wish to have included in their dossiers will have to be "blanked". Stringent

security measures were also set forth by the DPA (physical separation of data archives, encryption, access logs to be kept for at least 24 months); furthermore, a data breach notification obligation was introduced with a 48-hour deadline as from detection of the breach.

Management of Public Administrative Databases
Stringent security measures were laid down by the DPA in a decision of August 2015 to introduce privacy-compliant mechanisms in the electronic sharing of data by public bodies. Additionally, all public administrative bodies (including schools, regions, provinces, municipalities, health care bodies) will have to notify the DPA of any data breaches that are likely to impact significantly the personal information held in their data bases – within 48 hours of becoming aware of such breaches. An ad-hoc data breach notification form was made available by the DPA on its website.

Codes of Conduct on Business Information Systems
After analysing the contributions received via a public consultation, the Garante approved the 'Code of Conduct on Business Information Systems'. In accordance with the general data protection principles, the Code is aimed at laying down rules on the appropriate use of business reliability information with particular regard to the reports containing information on entrepreneurs and managers. Rules on transparency, data quality, relevance, accuracy are set forth by the Code which, according to Section 12 of the Italian Data Protection Code, is legally binding since compliance with its rules is a precondition for the processing of personal data to be lawful, and any breach may carry sanctions plus the payment of damages.

Processing of Employees' Personal Data
Several decisions were adopted in relation to the processing of employee's personal data. In a case, the DPA decided against the processing performed by a local police consortium, which relied on video surveillance systems deployed on their car fleet plus geolocation of the palmtop devices provided to their employees. The Garante banned location-based processing, which ultimately enabled all the operators to access several data items relating to their colleagues, because it was excessive and unnecessary for the purposes at issue as well as being in conflict with the safeguards set forth in Italy's law on workplace rights ('Statuto dei lavoratori').
By the same token, the Italian DPA found that the processing of personal data related to the browsing of the Internet by the employees of a marketing communications company was unlawful and accordingly prohibited the company from continuing that processing. Network traffic was monitored without informing employees and in the absence of a policy setting out the standards for employees' use of electronic devices; the monitoring allowed the employer to track down who was using which device.
Finally, a company was ordered to immediately terminate the processing of personal data relating to Skype-based conversations between an employee and third parties, as this was found to be in breach of the laws protecting confidentiality of communications as well as of the Guidelines issued by the DPA in 2007 and the company's own privacy policy.

Smartphone Location for Missing Persons
The DPA authorized two new geolocation techniques to rescue missing individuals in mountain areas. The smartphone location info will be transmitted to a dedicated operating centre (run by the National Alpine Rescue Service) irrespective of the given telecom provider's network in the vicinity of the missing person and without the individual's consent – but only after a search and rescue order has been issued formally by the competent authorities (fire brigade, police, health emergency services). The location info will only be processed for as long as necessary to locate the missing individuals and exclusively for the purpose of safeguarding their physical integrity and/or vital interests.

Public Consultations - IoT (Internet of Things) and mobile ticketing
In May 2015, a public consultation was launched on the Internet of Things (IoT) to gather suggestions and proposals on data protection issues with regard to the interaction and interlinking of networked things and devices; this was aimed ultimately to develop guidance enabling users to stay in control of their data – in particular, measures that can enhance transparency for users and protect them against the misuse of their personal data. More specifically, the DPA sought inputs on how best to inform users also with a view to obtaining their consent, where appropriate; on the mechanisms to foster privacy-by-design approaches by the industry; the application of encryption and anonymization techniques; mechanisms to ensure service interoperability and data portability; the adoption of certification tools.

A public consultation was also launched on a draft general scope decision concerning the processing of personal data in connection with mobile ticketing; the consultation was aimed at gathering inputs to develop a coherent set of measures to protect users and ensure the appropriate handling of personal information in this context. The draft measures [which were adopted formally at the beginning of 2016] envisage stronger safeguards and increased security when paying via one's mobile device for public transportation tickets, parking spaces, car-sharing or bike-sharing services or other traffic-related services – whether by direct carrier billing or via other channels (e.g. credit card debiting).

Online Profiling Guidelines
Guidelines published officially in May 2015 set out the legal requirements for online profiling as related to the most diverse services - from search engines to emailing, from social networks to e-payments and cloud computing. The guidelines are meant to afford protection to all users of online services, whether authenticated (e.g. email accounts) or non-authenticated. In order to profile users by processing their personal data to provide customized services and/or serve targeted ads, companies will have to make available exhaustive, clear-cut, and visible information starting from the home page, and this information should preferably be provided according to a layered approach. The guidelines clarify that any processing operation for profiling purposes, i.e. for purposes other than the provision of the specific service, may only take place on the basis of the users' informed consent and users may withdraw it at any time. This applies to all kinds of profiling, whether based on the scanning of emails or the combination of data collected from various features or services – including profiling via identification tools other than cookies (such as fingerprinting tools). Data retention issues were also tackled in the Guidelines, which require specific retention periods to be set out by having regard to the specific purposes sought in the individual cases.

Google's Privacy Policy – Visit at Google's Headquarters
Pursuant to a 'Decision Setting forth Measures Google Inc. Is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code' - adopted by the Garante in July 2014 - and the verification protocol submitted by Google and approved by the Italian DPA, a visit was carried out in the second week of May 2015 at Google's headquarters in Mountain View (CA) to assess the ongoing implementation process as for the measures set out by the Italian DPA (whose deadline was set at 16 January 2016). Those measures concern three main issues: 1) ensuring meaningful transparency and information to users; 2) developing consent (opt-in) mechanisms in line with European (and Italian) legislation, with particular regard to profiling and data combination across Google's multiple functions; and 3) clarifying the data retention and deletion policies followed by Google. The meeting allowed tackling several aspects on which in-depth exchanges of views were held with Google's engineering and legal teams and it led to Google's renewed commitment towards meeting specific, additional requests made by the DPA. Additional issues were raised such as Google's automated processing of emails (email scanning policies), anonymization policies and the need for more specific information, and the timescale for the European deployment of Google's ad controls.

Case-law

- *Court of Cassation – data disclosing sex life posted online by an employee*

The Court of Cassation (by judgment no. 17440/2015) fully confirmed the decision adopted by the Garante in a case of video surveillance carried out by a private company. Elaborating from the notion of personal data set forth in Article 4 of the Italian Data Protection Code, the Supreme Court clarified that an image is a personal data irrespective of whether the person portrayed is a famous one or the data controller can relate the image specifically to a person via tagging or other methods enabling identification of that person.

ICELAND / ISLANDE

Information on Major Developments in the Data Protection Field
July 2015 – June 2016

New Director General of the DPA
The Minister of the Interior appointed Mrs. Helga Þórisdóttir as the Director General of the DPA for a term of five years, beginning 1 September, 2015.

General Data Protection Regulation (GDPR)
The Ministry of the Interior has set up a working group which will oversee implementation of the GDPR through the EEA agreement, assess the need to modify national legislation, prepare proposals for new national legislation and analyze the effects on the Icelandic DPA. The DPA will participate in the working group.

The DPA has asked for a significant budget increase due to the implementation of the new GDPR so that the DPA can hire five specialists in order to keep up its current functions and principal activities as well as prepare for the GDPR simultaneously. Decision with regard to that has not yet been taken by the Ministry of the Interior.

Public Awareness
In order to raise data protection awareness, the Icelandic DPA has organised events, given presentations on data protection at various venues, and encouraged media coverage of data protection-related issues. The aforementioned events include the following:

European Data Protection Day – 28 January 2016
The DPA held a conference together with the University of Iceland‘s Human Rights Institute, on the Processing of Personal Data in the Private Sector and the Public Sector. The event brought together representatives of the Ministry of the Interior, the Prime Minister´s Office, the Federation of Trade & Services, and MP‘s. The DPA introduced general principles on data protection with regard to processing by companies and governmental bodies. The new GDPR was also introduced and its main goal to strengthen individuals‘ right to control over their own data.

UT-messan – 5-6 February 2016
UT-messan is one of the largest IT events in Iceland and its purpose is to highlight the importance of information technology and its effects on individuals, businesses and Icelandic society alike. The event includes a whole day conference for the IT industry, where the Director General of the DPA gave a presentation on Data Protection and the Internet of Things.

Annual Conference of the Legal Community – 15 April 2016
On 15 April, the DPA gave a general presentation on the new GDPR, and how its provisions affect controllers in particular, in a special plenary on data protection in regard to the digital revolution of the information society. The presentation took place at an annual conference held by the Icelandic Bar Association, the Icelandic Lawyers‘ Association and the Association for members of the judiciary.

Nordic Data Protection Authorities‘ Meeting – 11-12 May 2016

In May 2016, the Icelandic DPA hosted a yearly meeting of the Nordic DPA‘s in Reykjavik, with participants from Denmark, Norway, Sweden, Finland and the Åland Islands. Topics of discussion included the Implementation of the new GDPR, and the DPAs‘ Internal Preparations for it, the DPAs‘ Financial Status and Independence, Pro-active Cooperation Between the Nordic Countries, Experience from Participation in Global Cross Border Enforcement Network, Commercial Use of Personal Data, Processing by Credit Information Companies, Data Protection in Working Life, Camera Surveillance after GDPR, Public Authorities‘ Processing of Personal Data after GDPR, Data Protection Officers in the Nordic Countries, Handling of Data Breach Notifications, Use of Clouds in the Public Sector, IT-Security Inspections, Processors‘ Use of Encryption, Companies‘ Use of Security Measures, State of DPAs‘ Technological Competency, and more.

Statistical Data

According to statistical data, during 2015 the DPA received a total of 1.754 new cases, including 81 formal complaints, 468 inquiries, 448 notifications on the processing of personal data, and 411 cases related to scientific research within the health sector. Other projects include reviews on parliamentary bills and ministry regulations, audits, consultations, and more.

Annual Report of the DPA

The Annual Report of the Data Protection Authority, which provides further information in relation to the activities of the DPA during 2015, will be available soon at the DPA's website, www.personuvernd.is (in Icelandic only).

IRELAND / IRLANDE

Report from Ireland on Major Developments

(June 2016)

Minister for Data Protection

In May 2016, Deputy Dara Murphy was reappointed as Minister of State with responsibility for European Affairs and Data Protection, with his brief expanded to include responsibility for the EU Digital Single Market. Minister Murphy's reappointment to the data protection brief reflects the importance attached by the Irish Government to this key area.

Awareness Raising Activities

Alongside continued implementation of the Government Data Protection Roadmap (detail below), there has been a significant programme of activities and events to promote discussion and awareness of the data protection area over the past year.

A number of these events have focussed on promoting awareness of data protection across the Public Service, with Minister Murphy hosting two information sessions for Irish Semi State Bodies and Local Authorities in July and November 2015 respectively. Representatives of the Office of the Data Protection Commissioner (ODPC) spoke at each of these events. It is intended that further sessions will be held for Semi State Bodies and Local Authorities over the second half of this year in relation to the EU General Data Protection Regulation (GDPR).

In addition, an awareness raising initiative for the Civil Service centred on International Data Protection Day in January 2016 was organised. Material was prepared and circulated to all Government Departments, giving an update on data protection developments, along with promotional material (including posters) for use by all Departments. Further activities in this regard include a presentation by the Data Protection Commissioner to Senior Civil Service Officials in relation to the GDPR and its implications for the public sector.

The Minister also spoke at and participated in a wide range of events in relation to data protection and to raise awareness of the Government's work in this area. These engagements include presenting to Ireland's National Statistics Board, speaking at the Irish Computer Society's annual conference on International Data Protection Day 2016 and presenting to 600 plus participants on the Irish Law Society's Massive Open Online Course on Data Protection in June 2016.

Implementation of the Government Data Protection Roadmap

As referenced above, there was significant progress over the past year in the implementation of the Government's Data Protection Roadmap which aims to ensure that Ireland's approach to data protection in the digital economy is 'best in class' globally. In particular:

- July 2015 saw the first meeting of the Government Data Forum. Chaired by Minister Murphy, the Forum brings together a range of experts from industry, civil society, academia (law, sociology, psychology) and the public sector to advise Government on the opportunities and challenges for society and the economy arising from continued growth in the generation and use of personal data.

In the first instance, the Forum has decided to focus on those areas of data protection that relate to the citizen and in this regard, the Forum launched its first research output on the data protection implications of smart city technologies for the citizen in January this year; this has received very positive feedback from stakeholders and more widely.

Other key issues being considered by the Forum include approaches to increase greater awareness of data protection amongst key groupings of citizens, particularly young people as well as preparations for the GDPR.

- There have also been a number of meetings of the Inter Departmental Committee on Data Related Issues which was established in February 2015. Chaired by the Minister of State, the Committee brings together representatives of all Government Departments to discuss key issues and share best practice in relation to data protection and the management of data. It has been agreed that the Committee will be the key vehicle for Government Departments in preparing for the GDPR.

Office of the Data Protection Commissioner

Resources and organisation

The doubling of the budget of the Office of the Data Protection Commissioner to €3.65m for 2015 facilitated the recruitment of new staff including legal, technical, audit and communications specialists as well as policy and administrative staff.

The further funding of over €1.1m allocated in Budget 2016, bringing the 2016 allocation to over €4.7m, has enabled further significant additional recruitment of specialists throughout the year, continuing to increase resources for the various functions of the Office including awareness, investigations, audits and compliance-related matters. By end 2016, the Office's staff complement will number over 60.

To complement the Office's Portarlington operation, a permanent Dublin base is being established, and it is expected that the Dublin team will move to its new premises this autumn.

In 2015, a Special Investigations Unit headed up by an Assistant Commissioner was established. The Unit carries out investigations on its own initiative (as distinct from complaints-based investigations) and where it identifies offending behaviour it will use the Commissioner's full range of statutory powers to progress its investigations to an appropriate conclusion. Where it is considered necessary to do so, the Special Investigations Unit will adopt a sectoral approach to its investigative work.

A technical forensics lab was also established to assist in carrying out technical investigations and audits.

The Office continued to pursue an engaged approach to interacting with the many tech multi-nationals based in Ireland, as well as other public and private sector organisations, ensuring compliance with the law and safeguarding individuals' data rights. Building awareness at national level around data protection compliance was a key objective and the Commissioner and senior management undertook an extensive programme of speaking engagements across many industry sectors, speaking at some 60 events.

Complaints

During 2015, the Office of the Data Protection Commissioner opened 932 complaints for investigation.

Complaints from individuals in relation to difficulties gaining access to their personal data held by organisations accounted for over 60% of the overall complaints investigated during 2015. With 578 complaints in this category, this represented a record high number of complaints concerning access requests.

Complaints in 2015 about unsolicited marketing communications under the Privacy in Electronic Communications Regulations (S.I. No. 336 of 2011) saw a decrease compared to recent years with a total of 104 opened for investigation. The Office is confident that its active prosecution strategy in this area has contributed to the overall decline in this category of complaint.

The Office prosecuted 4 entities for a total of 24 offences under the Data Protection Acts of 1998 and 2003 and the Privacy in Electronic Communications Regulations of 2011.

In 2015 the Commissioner made a total of 52 formal decisions on complaints, 43 of which fully upheld the complaint

Data Security Breaches

In 2015, the Office of the Data Protection Commissioner dealt with 2,376 Data Security Breach notifications. This is an increase of 112 notifications compared to the previous year.

Audits

The Office of the Data Protection Commissioner undertook 51 audits and inspections during 2015.

Just under half of these, or 25, were unscheduled inspections carried out under section 24 of the Data Protection Acts. The aim of these audits and inspections is to check for compliance with the Data Protection Acts and assist the data controller in ensuring that their data-protection systems are as effective and comprehensive as possible.

The annual audit programme is tailored to focus on a number of carefully selected sectors. In 2015 the Office concentrated on recruitment practices as part of a wider investigation into enforced subject access requests. Also selected for closer examination was the deployment of CCTV in a range of shopping centres and retail outlets and a comprehensive review of the data-protection policies and procedures in three utility companies. In terms of the public sector, with the 2016 General Election imminent, an audit was conducted of Dublin City Council's Franchise Section. The Road Transport Operator Licensing Unit (Department of Transport, Tourism and Sport) was also audited in 2015.

In addition, a desk-based audit of 18 mobile apps was conducted as part of a Global Internet Privacy Sweep focusing on websites and apps either targeted at or popular among children.

LIECHTENSTEIN

Country report

Principality of Liechtenstein

Legal developments

Several contributions from the Data Protection Office were incorporated in the draft of an Act on the automatic exchange of tax data (AIAG). Te revised directive 2014/107/EC contains some additional privacy provisions, which were not included in the original directive 2011/16/EC (administrative cooperation in the field of taxation). Although Liechtenstein was not (yet) been formally committed to adopt these rules, the Data Protection Office suggested to implement them and were, subsequently almost fully taken over. By taking these rules into account, the rights of affected persons were strengthened. Finally, in the Act relating to the automatic exchange of tax related data a data breach notification duty was introduced The Act entered into force as of 1st January 2016.

Several articles of the Act of the Financial Intelligence Unit (FIUG) were amended and entered into force in Mai 2016. For example, provisions regarding data retention and deletion as well as an indirect right of access were included into the law. Due to the mentioned new provisions of the FIUG the Data Protection Office has to fulfil new tasks.

Other developments

As mentioned above, the automatic exchange of tax related data has been on top of the agenda of the Data Protection Office. In Liechtenstein, the Data Protection Office participated in a consultative group set up by the Government to address the topic.

As a consequence of the Digital Rights judgment of the CJEU, a working group was set up by the Government to analyse the possible consequences for the legal situation in Liechtenstein. Work is on-going.

The Data Protection Office followed the ongoing work concerning the data protection reform in Brussels and Strasbourg within the given resources.

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 *"Wired and sold! Who determines my digital self?" (Verdatet und verkauft! Wer bestimmt über mein digitales Ich?)*

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

LITHUANIA / LITHUANIE

33RD PLENARY MEETING OF THE COMMITTEE THE CONVENTION 108
STRASBOURG, 29 JUNE – 1 JULY, 2016
COUNTRY REPORT – LITHUANIA

---

1. Recent National Developments – legal framework

1.1. No changes of the Law on Legal Protection of Personal Data of the Republic of Lithuania related to the use of technologies since year 2011, when the last changes have been made.

1.2. Legal Acts on implementation of the Law on Cyber Security of the Republic of Lithuania have been issued by the Government of the Republic of Lithuania

1.2.1. The Resolution of the Government of the Republic of Lithuania No 422 of 23 April 2015 on Establishment of the Cyber Security Council and the Approval of its' Working Rules and Procedures has been approved by the Government

The Cyber Security Council has been established seeking to ensure proper implementation of the Law on Cyber Security of the Republic of Lithuania and to develop cyber security standards as well as enforce public and private sector to implement them in practice. One of the targets also to encourage academic society focus on education of a staff of owners of the critical infrastructure. The Council consists of twenty four members. These are representatives of National Cyber Security Centre, CERTs', Ministry of National Defence of the Republic of Lithuania, Power plants, Kaunas Technology University, operators of electronic communications networks. Rita Vaitkevičienė, Deputy Director of the State Data Protection Inspectorate of the Republic of Lithuania is also the member of the Council. She is authorised to delivery opinion on monitoring of the activity of electronic communications services and public communications networks providers, handling of the information about cyber incidents when these incidents is likely to adversely affect the personal data or privacy of an individual and on carrying out investigations in case of personal data security breach.

1.2.2. The Resolution of the Government of the Republic of Lithuania No 87 of 25 January 2016 on the Approval of the National Plan on Management of Cyber Incidents has been approved by the Government

National Plan on the Management of Cyber Incidents lays down an obligation of CERTs and other entities who have responsibilities under the Law on Cyber Security to appoint contact person and the staff who will respond to cyber incidents, establishes classification criteria of incidents, procedures of responding and investigation of incidents and etc. A simulation of cyberattack and the training is planned on the end of September 2016.

2. Case law

2.1. The explicit purpose in an agreements on the data transfer

The SDPI received a complaint that civil servant of the Municipality N sent a request to the Real Property Register asking data about all immovable property of the applicant for the purpose of allocation of an address to a household (dividing up of land). During investigation SDPI founded that above mentioned purpose is not included in the agreement between Municipality N and the Real Property Register. The SDPI issued an order to the Municipality N which was appealed by that Municipality to the Vilnius Regional Administrative Court. The Court annulled an order of the SDPI. SDPI appealed to the Supreme Administrative Court with request for annulment of that Court Decision. The ruling of the Court is that any data might be collected only if it is written in the agreement between parties.

2.2. Sending of documents by fax

The SDPI received a complaint that advocate sent an information about Complainants' debts to the office of' his employer by fax. The Court decided that such disclosing of data do not correspond requirements of Article 30 of the *Law on Legal Protection of Personal Data.* The SDPI draw up the Protocol of Administrative offence and sent to the District Court of Vilnius Region. The Court decided that advocate violated Article 30 of the Law on Legal Protection of Personal Data and he shall be fined. The decision was appealed by the advocate to the Vilnius Regional Administrative Court and having ruling of II instance to the third instance – Supreme Court of Lithuania. The advocate stated that sending by fax is not processing of data. Supreme Court of Lithuania decided that any operation carried out with personal data: collection, recording, accumulation, storage, classification, grouping, connecting, changing (supplementation or correction), provision, publication, use, logical and/or arithmetical operations, search,

dissemination, destruction or any other action or set of actions is data processing so sending of data by fax is data processing also and disclosure of personal data of the person to his employer is violation of the laws. .

3. Investigations on SDPI initiative

3.1. Video surveillance in labour exchanges

Seeking to clarify lawfulness of the processing of personal data of jobseekers and unemployed SDPI carried out inspections in 11 labour exchanges and found that 5 of them violated the Law and instructions as regards possible remedy the infringements found.

These and other preventive inspections carried out by SDPI can be found on the website, the address: *http://www.ada.lt/go.php/lit/Patikrinimu-rezultatu-apibendrinimai/321/1 (in Lithuanian only)*.

3.2. Personal Data Protection at the working place

Following the decision of Estonian, Latvian and Lithuanian data protection supervisory authorities to check lawfulness of employees' data processed by administrations of big supermarkets (malls) SDPI executed coordinated inspections in supermarkets of 4 biggest retail networks. In all cases have been found violations of the laws, summary is published in the website, the address: *http://www.ada.lt/go.php/lit/Patikrinimu-rezultatu-apibendrinimai/321/ (in Lithuanian only)*.

3*. Public awareness*

4.2. Recommendations on personal data protection for use of devices with Android applications

Each actionable email address, scanned copies of the photos and documents found on the internet might be misused for a purpose of obtaining benefit as a result of crime. To help people, especially users of devices with Android applications, understand how to protect personal data and to ensure the confidentiality of communications by using these devices SDPI issued recommendations, the address is *https://www.ada.lt/go.php/Valstybines-duomenu-apsaugos-inspekcijos-rekomendacijos122122 (in Lithuanian only).*

4. *Other*

5.1. An Order of the Director of the State Data Protection Inspectorate of the Republic of Lithuania No 1T-31 (1.12.) of 22 July 22 d. 2013 On Electronic Administrative Services Provision has been supplemented

The State Data Protection Inspectorate implemented IT project which allows collect applications and delivery administrative services via electronic service portal or e-mail box service provided by Lietuvos Pastas *(Lithuanian Post*). Applicants have possibility to delivery applications and receive responses in electronic form. The Order of the Director of the Republic of Lithuania No 1T-31 (1.12.) of 22 July 22 d. 2013 On Electronic Administrative Services Provision has been supplemented on Year 2015 and Decreasing of the administrative borders stipulated significant increasing of enquires (Inspectorate received three times more applications for indirect access to personal data).

MALTA / MALTE

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD

Summary of activities and news

During the year under review, the Office's workload continued to increase in a constant pattern. Insofar as complaints are concerned, the Office received numerous complaints where citizens felt their privacy was being threatened and therefore resorted to a remedy before the Information and Data Protection Commissioner. The most common subjects of these complaints referred to unsolicited communication via e-mail or text messages and disclosure of personal data without the data subject's consent. As part of the investigation of a number of the complaints received, this Office conducted inspections with the relevant data controllers in order to ascertain the veracity or otherwise of the alleged facts made in the respective complaints.

After the termination of Mr Joseph Ebejer's term serving as Information and Data Protection Commissioner, who did not seek re-appointment, Mr Saviour Cachia was appointed as his successor. Mr Cachia, a long-time seasoned civil servant, was actively involved in the transposition of the Data Protection Directive in the Maltese body of laws and following its enactment, was commissioned to identify a strategy to implement the Act at national level. Prior to this appointment Mr Cachia was responsible for the management of a corporate project to implement data protection compliance in the Public Service, incorporating all line ministries and government departments. He participated in various Data Protection conferences while in this capacity and as a consequence is well known in the data protection circles both nationally and also on a European level.

Insofar as legislative developments and interventions are concerned the Information and Data Protection Commissioner launched an initiative to set up a working group on 'Data Protection and Education' with the main objective of looking into and analysing the processing of personal data for education purposes and ultimately proceed to develop a report followed by a legal instrument under the Data Protection Act in order to better regulate the processing of personal data in the Education Sector at all levels. This working group was constituted with representatives of education authorities, educational institutions (ie: state, church and independent schools) as well as post-secondary and tertiary educational institutions. The report and legal instrument were finalised within a few months of the set-up of the working group and it was eventually decided to adopt the legal instrument as a subsidiary legislation under the Data Protection Act. The legal instrument was adopted in 2015. It *inter alia* regulates the processing of students' personal data by both education authorities and education institutions and provides amongst others for the use of such data for research and statistics purposes. The use of pseudonymous data as a relatively new concept was also introduced in the same regulations.

Awareness raising initiatives were taken during this year which included amongst others participation in seminars on data protection, local radio programmes with phone-ins and television programmes and when requested, interviews to newspaper journalists. These initiatives also included the proactive approach of meeting the various sectors within the local industry with the firm objective to discuss their business operations and address any arising data protection issues or concerns which might necessitate an intervention by the Commissioner. This Office adopts the approach of coordinating such meetings with the widest representation possible of the respective sectors. This approach proves to deliver satisfactory

results particularly where guidelines or codes of practice need to be developed in order to regulate specific areas within the sector.

During the period under review, the Office continued to honour European and international commitments by participating in various data protection fora.

MONACO

PRINCIPAUTE DE MONACO
Développements majeurs intervenus en matière de protection des données personnelles
Période allant de juin 2015 à juin 2016

*****

Lois

Loi n.°1.420 du 1 décembre 2015 portant modification des articles 18 et 19 de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée.
Cette loi rétablit les pouvoirs d'investigation de la Commission de Contrôle des Informations Nominatives qui avaient été jugés inconstitutionnels par trois décisions du Tribunal Suprême en date du 25 octobre 2013.

Ordonnance Souveraine

Ordonnance Souveraine n°5.664 du 23 décembre 2015, créant l'Agence Monégasque de Sécurité Numérique en charge de la sécurité des systèmes d'information et placée sous l'autorité du Conseiller de Gouvernement-Ministre de l'Intérieur.

Arrêté Ministériel

Arrêté ministériel n°2016-59 du 28 janvier 2016 modifiant l'arrêté ministériel du 4 février 1947 portant règlement des prestations médicales, chirurgicales et pharmaceutiques allouées aux fonctionnaires, modifié.

Circulaire

Circulaire n°2016-02 relative à l'information des assurés relevant du service des prestations médicales de l'Etat sur le respect de la protection des informations nominatives exploitées par ce service.

Projets de loi

Projet de loi n° 934 relative à la lutte contre la criminalité technologique.

Projet de loi n° 944 portant diverses mesures relatives à la préservation de la sécurité nationale.

Projet de loi n° 945 modifiant certaines dispositions relatives à la Médecine du Travail.

Autres dispositions

Signature par Monaco de l'Accord Multilatéral entre les Autorités Compétentes, destiné à faciliter l'échange d'information entre ses signataires et qui contient des dispositions en matière de confidentialité et protection des données signée le 15 décembre 2015 et complète la Convention signée en octobre 2014.

Paraphe le 22 février 2016 du protocole avec l'Union Européenne qui utilise également la Norme d'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale établie par l'OCDE et prévoit des dispositions en matière de protection des données personnelles.

Evaluation en cours de Monaco par l'OCDE en matière de protection de données et de confidentialité en prévision de l'échange automatique (résultat connu en juillet 2016).

Intégration de l'autorité de contrôle dans le groupe de travail mis en place pour la mise en œuvre de l'échange automatique d'informations en 2018.

Recommandations CCIN

Recommandation n° 2015-111 de la Commission en date du 18 novembre 2015 qui annule et remplace la délibération n° 2015-119 du 16 juillet 2012 et encadre de façon plus précise les traitements de messagerie électronique mis en place à des fins de surveillance ou de contrôle.

La recommandation n° 2015-113 de la Commission en date du 18 novembre 2015 qui annule et remplace la délibération n°2012-24 du 13 février 2012.
L'objectif de la Commission est d'appeler l'attention des responsables de traitement sur l'utilisation qui peut être faite des copies de documents d'identité afin notamment de prévenir les risques d'usurpation d'identité.

Brochure diffusée à l'occasion de la 10ème journée de la protection des données
A l'occasion de la 10ème journée de la protection des données la CCIN a adressé aux organismes publics et privés de Monaco (3.400 entités au total) une brochure de sensibilisation à la protection des informations nominatives, indiquant notamment les formalités à accomplir auprès d'elle.

POLAND / POLOGNE

T-PD

Country report on major developments in the data protection field

I. Legislation

1. Data protection law

As of 1 June 2016 amendment to the Act of 29 August 1997 on Personal Data Protection entered into force. The changes to the above Act were introduced by the Act of 18 March 2016 amending the Act on the Commissioner for Human Rights and certain other acts. The changes relate to the immunity of the Inspector General for Personal Data Protection and consist in adding the provisions of Art. 11a-11g.

On 1st April 2016 the Act on state help in child raising came into force. It introduced important changes in data protection act with relation to data controller as well as subcontracting of data processing operations.

Amending act contains, among others, provisions stating that:

state institutions, local government institutions as well as dependent entities shall be treated as one data controller, provided that data processing is carried out in the same public interest; and

an agreement between data controller and processor is not required, where controller and processor are entities that represent state institutions, local government institutions or dependant entities.

The Inspector General has signalled its objection against the aforementioned provisions, indicating that they are not in compliance with the Directive 95/46/EC. This opinion however, has not been taken into account. Therefore, the Inspector General, being the keeper of proper, high standard of personal data protection in Poland, will interpret introduced amendments, having in mind the provisions of the Directive 95/46/EC, referring to the jurisprudence of the Court of Justice of the European Union, which states that in case of wrong implementation of directive it is possible to the entities in the course of court proceedings to directly refer to the wording of directive. Simultaneously, having in mind that the approach presented in the aforementioned amendment is at variance with binding European law, the Inspector General for Personal Data Protecting will strive for change of this act.

2. Amendment to the Police Act and any other government services

On 7th February 2016 in spite of many reservations formulated, among others by GIODO, Commissioner for Human Rights, National Council of the Judiciary as well as attorneys and counsellors, the amendment to the Act on police and special services came into force.

This amendment ought to implement the Constitutional Tribunal judgment of 2014, by virtue of which, the provisions on disclosure of telecommunication data to police and special services without independent, external supervision have been declared as incompliant with the Constitution.

The amendment introduces a rule, according to which, a competent local court is entitled to control ex ante, acquisition of telecommunication, postal and Internet data. To this end, empowered entities have to pass on to the Court, once every six months, report on number of requests for data disclosure. The court, if it wants, can consult reasoning of requests for data disclosure.

In GIODO's opinion, such form of supervision is insufficient and it results in lack of real supervision over the actions of services. GIODO remarks concerned the fact that there are to many situations in which special services could acquire telecommunication data as well as lack of information obligation with relation to individuals (ex ante) on operational actions taken with relation to them as well as on collected information relating to those individuals.

In its reasoning GIODO stated that the amendment is not in line with guidelines of the Court of Justice of the European Union, presented in its judgment of 8th April 2014 in joint cases C-293/12 and C-594/12 Digital Rights Ireland, where the Court declared the Directive 2006/24/EC on data retention invalid. As stressed by the Court, the directive did not establish an objective criterion guaranteeing that competent national institutions would have access to data and could use them only for the purpose of preventing, detecting and prosecuting of crimes sufficiently serious to justify such type of measures. Mere reference to notion of "serious crimes", established in law of Member States, is insufficient in the light of proportionality requirements.

II. Inspection activity

1. Misuse and wrong interpretation of consent to data processing.

Inspections conducted by GIODO have shown that data controllers try to get consumers consent to disclose their data to other entities for the purpose of marketing activities. Findings of one of the inspections showed that data controller collecting data for the purpose of marketing activities requested that data of the company and third entities can be processed for the purpose of promotion, advertising and marketing. Basing on consent, data controller not only has used those data for marketing of its own products and products of other companies, but also disclosed them to other entities which use them for their own marketing purposes. An administrative proceedings has been commenced with relation to this controller. It has been ultimately remitted, due to the reestablishment of proper legal state by the controller.

2. Illegal processing of biometric data

On 16th December 2015 the Voivodeship Administrative Court dismissed complaint of a company against the Inspector General's decision, maintaining in force its decision of 6th November 2014, by which the Inspector General ordered an entity running fitness club to cease processing of biometric data of its customers without legal basis. The prior inspection had showed that the system of biometric check had been established in some clubs. This check was performed through entrance gate, by which fingerprint of a person was read and compared to the biometric code recorded on band, being at the same time an entrance ticket. The Court agreed in its judgment with GIODO's position and deemed that customers data as well as biometric code assigned to them constitute personal data. The court has not recognised an explanation, according to which the processing of biometric data was necessary in order to execute an agreement.

III. eGovernment

1. Strategic directions of the actions of the Ministry of Digital Affairs in the field of digitalisation of public services.

On 15th February 2016 the Minister of Digital Affairs declared a strategy in the field of digitalisation of public services. The strategy pursues the aim comprising:

possibility of handling any case that touches upon public administration at any level, through electronic means;

no need to know complicated structure of Polish administration;

no need to disclose the same data many times;

possibility to handle all cases through one, clear website dedicated to e-administration; and

introduction of verified method of secure identification and payments.

It has been also agreed that the implementation of aforementioned goals requires implementation of several strategic changes focused around five rules:

The State shall serve the citizen. Due to the digital technology it shall combine dispersed institutions and convert complex procedure into simple and coherent services;

Access to Internet and public services has to be secure to our data and to all types of transactions made on the Internet;

In order to fulfil the aims of e-administration, but above all to fulfil social and economic goals, it is prerequisite to speed up the development of modern telecommunication infrastructure;

The development of innovative economy requires on-going, easy access to data collected by public services;

We need to constantly, regardless of age, improve our digital skills, in order to effectively use the advantages of digitalisation and to compete on the global market.

2. Electronically supplied services

In 2015 GIODO launched new electronically supplied services which facilitate citizens' contact with the DPA. These services ensure the possibility to send required letters and notifications to the GIODO Bureau exclusively electronically with the use of electronic identification services. In the reporting period, forms were launched dedicated to notifying appointed DPOs to GIODO pursuant to the national provisions. Additionally, in GIODO's information service constituting a public register of appointed DPO's, a service destined for issuing confirmations proving appointment and notification of DPOs was launched, which simplified previously applied administrative actions in this regard based on issuing such confirmations on the basis of received applications. Currently, data controllers can print such confirmation at any time without the need to file applications.

In the reporting period, GIODO Bureau drew up as well a description of all cases handled in the Bureau and uploaded it in the ePK service (https://www.biznes.gov.pl/organy-i-instytucje/-/szczegoly/45), which constitutes a guide in different language versions for entrepreneurs conducting economic activity in Poland. This service constitutes at the same time the execution of the provisions of the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, which provides for creation of "points of single contact". The recommendations of the above Directive concerning creation of points of single contact were introduced into the Polish law by the Act of 4 March 2010 on Provision of Services in the Territory of the Republic of Poland, which introduced into the Act of 2 July 2004 on Freedom of Economic Activity chapter 2a entitled "Point of contact". The amendment entered into force on 10 April 2010. Independently from the description of all procedure realised by GIODO, ePK service launched the procedures most often used by users in online version, directly accessible from this service or from electronic service of the GIODO Bureau called eGIODO.

IV. Combating a criminal offence against bank systems

On 15th April 2016 the Police informed on detection and disruption, together with National Public Prosecutor's Office, of an international, organised crime group, acting in the field of money stealing through breaking on-line to bank accounts and transferring money with the help of TIMBA virus. Loses are estimated at 94 million PLN, whereas retrieved sum amounts to 57 million PLN. Up to now, charges have been made against 148 suspected citizens of Poland and Latvia, concerning over 850 deeds. On the territory of Denmark and Poland three Polish leaders of this group have been seized. Two o them were prosecuted through European Arrest Warrant. All of them used forged documents. The group acted in Poland, Denmark, Great Britain, the Netherlands, Italy, Slovakia, Czech, Austria, France, Hungary, Bulgaria, Croatia, Spain, Montenegro and Germany. The group was disrupted due to the cooperation of law enforcement authorities, Polish Bank Association, General Inspector of Financial Information, CERT NASK, Europol and Eurojust.

V. Events

In 2016, just like in previous years, GIODO celebrated, already for the 10th time, the European Data Protection Day. As each year, conferences devoted to most recent issues related to the right to privacy and data protection were held, however this year GIODO invited to their co-organisation universities with which it concluded cooperation agreements, and so the events organised within the framework of those agreements at the premises of the universities included:

13 January 2016, Katowice - the Conference on "The protection of medical data" organised by the University of Silesia in Katowice in cooperation with GIODO;

14 January 2016, Dabrowa Gornicza - Open Day organised at the premises of the Academy of Business, including the possibility to obtain legal advice and information on personal data protection, as well as the Conference on "Current problems of personal data protection in direct marketing services";

19 January 2016, Szczytno - the Conference on "Identity theft" organised by the Police Academy in Szczytno in cooperation with GIODO;

19 and 20 January 2016, Lodz – legal advice on personal data protection provided by GIODO's representatives at the Faculty of Law and Administration at the University of Lodz;

28 January 2016, Warsaw – as the main event on the occasion of the Data Protection Day GIODO organised with the University of Warsaw the Conference entitled "The protection of personal data in the era of Big Data". The possibility to obtain legal advice on personal data protection provided by GIODO's representatives;

23 February 2016, Warsaw – the Conference devoted to the new role and position of Data Protection Officers organised by GIODO with the Kozminski University at the premises of the latter;

25 February 2016, Warsaw – the Conference on the processing of personal data by churches and religious associations organised at the Cardinal Stefan Wyszynski University.

Also, on 2 February 2016 GIODO traditionally organised, for the tenth time, the celebration of the 10th Data Protection Day, in cooperation with and at the premises of the Permanent Representation of the Republic of Poland to the EU, in Brussels. The celebration was attended by Data Protection Commissioners of the EU Member States, 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.

Furthermore, in January/February 2016 the Data Protection Day events were organised by teachers vocational training centres, primary, middle and secondary schools all around Poland within the framework of the Poland-wide Educational Programme „Your Data – Your Concern", which is realised by GIODO. The activities undertaken at the local level by participants of the Programme are aimed at raising awareness of the protection of one's privacy and personal data among the entire school community and local environment.

VI. GIODO projects and programmes

Within its educational activity, GIODO is inter alia involved in realising two projects co-funded by the Fundamental Rights and Citizenship Programme of the EU. The first one is the ARCADES project (Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union) realized by GIODO as coordinator in cooperation with the Slovak and Hungarian DPAs and Vrije Universiteit Brussel in 2014-2016. The concept of the project is based on the Poland-wide programme "Your data – your concern". Its aim is to introduce at schools in the EU the data protection and privacy related content to shape informed and responsible attitudes towards data protection and privacy among school children and teens (6-19 years old). Also a publication is being developed presenting the project's results (a unified set of teaching aids - data protection principles, lessons' scenarios, etc.) entitled 'The European Handbook for Teaching Privacy and Data Protection at Schools'.

The second one is the PHAEDRA II project (Improving practical and helpful cooperation between data protection authorities II), being a continuation of the PHAEDRA I project implemented in the years 2013-2015 in cooperation with Vrije Universiteit Brussel (project coordinator), UK Trilateral Research & Consulting LLP (partner) and Spanish Universitat Jaume I (partner). PHAEDRA II is focused on identification, development and recommendation of the measures for improving practical cooperation between European Data Protection Authorities (DPAs). The main area of investigation is aimed at identification of the factors improving cooperation between these authorities, especially in the context of the reform of the data protection framework proposed by the EC. The project will deliver practical instruments and mechanisms improving cooperation between DPAs, as well as it will elaborate the operational legal guidance. It tackles three of the biggest challenges facing European DPAs: ensuring consistency, sharing different types of information (including confidential) and coordination and cooperation regarding enforcement activities.

VII. Agreements on cooperation

On 22 September 2015 GIODO concluded the Agreement on cooperation on the protection of privacy and personal data with the Commandant-in-Chief of the Polish Police and the Higher Police School in Szczytno. The cooperation comprised joint undertakings in the field of research and scientific, educational, promotional, publishing and training related activity as well as with regard to execution of DPO's tasks.

On 5 November 2015 GIODO concluded the Agreement on cooperation on the protection of privacy and personal data with the Faculty of Law and Administration of the University of Warsaw. The agreement relates inter alia to research, educational, publishing and promotional cooperation.

In 2016 GIODO concluded agreements on cooperation on the protection of privacy and personal data with the following institutions: the University of Silesia in Katowice (13 January), the Cardinal Stefan Wyszynski University in Warsaw (25 February), the Nicolaus Copernicus University in Toruń (5 March), the Polish Chamber of Commerce (10 May), the Polish Naval Academy in Gdynia (23 May), the University of Gdańsk (24 May).

SLOVAK REPUBLIC / REPUBLIQUE SLOVAQUE

The Office for Personal Data Protection of the Slovak Republic,
Hraničná 12 820 07 Bratislava

A. General review

We live in the digital era of social media which are widely used not only by adults but also by minors. Therefore, the central theme in the work of the Office for Personal Data Protection of the Slovak Republic (The Office) in 2015 was protection of personal data of minors. This agenda was discussed in the meetings with the representatives of executive, legislative and independent public bodies such as the Office of the President of the Slovak Republic, the Human Rights and Ethnic Minorities Committee of the National Council or the Office of the Public Defender of Rights as well as publicly presented in the media. The President of the Office especially accented the special role of education in the prevention of abuses of minors.

The preparations for the Slovak Presidency in the Council of the European Union (SK PRES) and the final works on the reform of data protection rules in the EU were also significant topics in the work of the Office in 2015. The efforts of the Office representatives and deputies were focused on the consultations and finalization of new General Data Protection Regulation (GDPR) at European as well as national level.

In 2015 the Office issued its opinion on the data subject's consent. This topic is of the special importance as it is frequently the matter of telephone, email or written requests from controllers, processors and data subjects. Therefore, the Office deemed it crucial to deliver the expert opinion elaborating the controllers' responsibilities as well as the components that should be present concerning the data subject's consent to process personal data fairly and lawfully.

The Office further continued in a weekly service of monitoring and assessment of materials in the legislative process within the inter-ministerial review proceeding. The aim of this process is to track all materials included in the inter-ministerial review proceeding and to effectively evaluate and comment on such materials. For that reason, every legislation draft that governs by its content processing of personal data must comply with the basic requirements of the Act on personal data protection. In 2015, the Office commented on 120 dossiers put forward for the inter-ministerial review proceedings what more than doubled the last year reported amount.

B. Decisions

The Office provided several expert opinions and consultations to other authorities, answered the great amount of questions in writing (70 requests), by phone (2000 requests) and email (380 requests) to public and provided approximately 70 replies to the media requests in order to provide more detailed information on data protection in specific cases, as well as actively participated in conferences and international meetings.

The Office issued 199 first instance decisions, from which 33 decisions were appealed. Concerning the second instance decisions the Office issued 24 decisions. As for the sanctions, the Office delivered 109 decisions on corrective measures and 26 decisions on penalties. Five decisions on penalties were appealed and in two cases the second instance upheld the first instance decision.

C. Notifications, prior checks, exams and inspections activities

The Office performed 637 exams of DPOs at the establishment of the Office and in other regions of the country for 707 applicants in total. The Office issued 543 certificates of successful completion of tests.

As much as 1275 notifications were filed by controllers in 2015 and 1187 confirmations of processing based on notifications were provided by the Office. 41 prior checks were filed by controllers in 2015 and 51 authorizations on the basis of prior checks issued by the Office.[1]

In 2015 the Department of Inspections conducted 19 regular and 90 exceptional inspections in all the regions of Slovakia.

D. Particular issues

The Use of CCTV

The Office anticipated the decision of the Court of Justice of the European Union ("CJEU") in the case C-212/13 František Ryneš v. Úřad pro ochranu osobních údajů resulting from the request for a preliminary ruling from the Supreme Administrative Court of the Czech Republic. The CJEU ruled that video surveillance which covers a public space cannot be regarded as an activity which is a purely personal or household activity meaning the exemption for "personal or household activity" does not permit the use of a home CCTV camera that also films any public space. The ruling confirmed the position of the Office and its decisions in these cases.

The data subject's consent

In 2015, the Office received several requests from data subjects, processors and controllers for the detailed information on the consent of data. The areas that were concerned the most were (home) CCTV cameras, processing of employee data, processing of health information and processing of personal data of minors. The Office dealt intensively with the cases of using CCTV which became more widely used in order to protect human life, health and/or property. For this reason, the Office issued numerous opinions on the consent of data subject in the individual cases as well as the guideline. It stressed that in order to process personal data fairly and lawfully either the consent of data subject or the other legal bases is necessary.

In view of the central theme in the agenda of 2015, the Office focused on the education and communication with the public. In order to improve the awareness about the minors' personal data protection, preparations for launching an email address to make reporting of any breaches of this kind to the Office easier and more accessible started. It was also decided that the protection of minors is the main topic of the upcoming Data Protection Day.

[1] This discrepancy in the number of confirmations and filings for prior check is due to the specific procedure in case of the processing of data for the purpose of protection of the rights the processor

SLOVENIA / SLOVENIE

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD IN 2015

Report by the Information Commissioner of the Republic of Slovenia

for Council of Europe, TP-D Committee

A. Summary of activities

The Information Commissioner (IC) is the inspection and offence authority in the area of data protection as provided by the Personal Data Protection Act of Slovenia (PDPA). In July 2014 Ms Mojca Prelesnik was appointed for a 5 year mandate.

In 2015 the IC initiated 791 cases regarding a suspected breach of the PDPA provisions, 343 in the public and 448 in the private sector. The IC also initiated 104 offence procedures. The procedures mainly concerned suspected violations in relation to direct marketing, personal data being published on the internet, video surveillance, automatic forwarding of work e-mails and unlawful access to them, and lack of data security. A problem that was identified in a number of procedures are data controllers offering their services online in Slovenia, but having only a letterbox company registered in Slovenia, which presents a big challenge to enforcement.

In addition to the inspection and offence authority competencies the IC performs other tasks as provided by the PDPA. It issues non-binding opinions and clarifications on specific issues regarding data protection raised by the individuals, data controllers, public bodies and international bodies. In 2015 the IC issued 3.369 opinions and clarifications (1.667 in writing and 1.702 clarifications over the phone). The high number may be attributed to the transparent work and intensive public campaigning. The IC is an appeal body regarding access to individual's personal data as well (100 cases in 2015) and was consulted by the legislator and competent authorities in the course of preparation of 98 Acts and other legal texts.

The IC also performs informal data protection impact assessments, as they are seen as one of the most important tools for early consideration of data protection aspects of a solution, technology, etc. In 2015 more than a 100 subjects from the private and public sector contacted the IC with such a request.

The IC is under PDPA also competent to conduct prior checks regarding biometric measures, transfer of data to third countries and connection of filing systems. The data controllers in such cases need to firstly obtain the IC's permission. In 2015 the landmark ruling on the invalidity of Safe Harbor agreement was issued by the European Courts of Justice, which had a big impact on data controllers exporting data to the US. The IC issued an administrative decision that Safe Harbor is not to be regarded as offering adequate level of data protection and was consequently faced with numerous questions regarding possibilities of lawful transfer of data to the US and applications for prior checks.

In terms of policy issues the IC has dealt with extensively, it is necessary to mention the digitalization of homes, cities and traffic infrastructure, involving smart, interconnected devices that have the capability to process extensive quantities of data and have a significant impact on the privacy of citizens (the concepts of internet of things and big data). Drones and the lack of legislation specifically regulating their use to ensure the protection of fundamental rights of individuals were also still a priority of the IC.

In the course of its awareness rising activities the IC continued its preventive work (lectures, conferences, workshops for different public groups). Together with the Centre for Safer Internet of Slovenia it covered awareness rising activities for children and young people (lectures at schools, publications). The IC also published a record number of guidelines on different data protection topics:

- Guidelines on video surveillance,
- Guidelines on contractual processing of personal data,
- Guidelines on the recording of telephone calls,
- Guidelines on data protection in relation to the use of GPS technology,
- Guidelines on the security of personal data,
- the IC had to update three existing guidelines in accordance with the decision of the ECJ on the Safe Harbour agreement:
    - Guidelines on the transfer of personal data to third countries,
    - Guidelines on the data protection in the context of cloud computing,
    - Guidelines on cloud computing for small business.
- The IC issued a report on the aspects related to the protection of human rights in the use of drones.

In the context of the European Data Protection Day the IC organized a round table debate dedicated to the elderly and issued a practical leaflet with advice on data protection related issues relevant for the people in retirement. On this occasion it awarded 2 data controllers for good practice in personal data protection – one of the awards being dedicated to the efforts for respect of Privacy by Design principle. Special awards have been issued to seven companies who have acquired the ISO/IEC 27001 standard for the information security management.

The IC also participated in a number of international bodies: The Article 29 Working Party, Joint Supervisory Body of Europol, Joint Supervisory Authority for Schengen, Joint Supervisory Authority for customs, EURODAC, International Working Group on Data Protection in Telecommunications, Council of Europe's Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). The IC was also active in the field of bilateral international cooperation. In 2015 it hosted study visits of the representatives from the DPAs from Montenegro and Kosovo.

In a consortium with partners from different EU Member States the IC worked on a 3 year project CRISP, which focuses on evaluation and certification schemes for security products. The Information Commissioner is also one of the partners in the European project ARCADES, that centres on inclusion of data protection and privacy protection topics in curriculums of primary and secondary schools in the EU.

B. Information on interesting case-law

1. Collection of personal data for the purposes of direct marketing based on clients' recommendations'

The IC initiated an inspection proceeding against a cosmetic salon which collected the personal data of individuals - potential clients (for the purpose of offering free testing of their products) based on questionnaire in which clients have listed personal data of third parties which they recommended as potential clients for the free testing (first name, family name, telephone number, age, occupation). The salon used the telephone number to conduct direct marketing activities – i. e. offering the free testing.

The IC concluded that the beauty salon had no legal ground for the processing of the above mentioned personal data of third parties (since the data have been collected without their consent or other legal basis). In addition the cosmetic salon has collected disproportional range of personal data since only the name and telephone number would suffice for the salon to establish first contact with a potential new client. Therefore the IC ordered that the above mentioned collection and processing of personal data from third parties without their explicit consent has to stop unless a client explicitly declares and proves that the third party has given consent for the disclosure of specific personal data to the cosmetic salon to be processed for the purposes of direct marketing and/or offering of free testing. It is namely the duty of the cosmetic salon as data controller to ensure and verify if the informed personal consent has been given by the third parties and to clearly inform their clients and enable them to obtain and demonstrate the existence of an unquestionable consent of third parties before their personal data is disclosed to the salon. The IC has ordered the cosmetic salon to delete any personal data on individuals collected in unlawful manner.

2. Conducting of video surveillance of public area

The IC initiated an inspection proceeding based on the suspicion of illegal conduct of video surveillance of areas of public use since it has been established that the local municipality has been conducting constant video surveillance of almost entire area of one of the main squares including local buildings. As it was established in the preceding the purpose of this video surveillance was assurance of the safety of people and property, as some important institutions (such as bank, post office), as well as municipality owned defibrillator, are located in the area under surveillance. The use of cameras proved also to contribute to greater safety in the area.

However the IC has also established in the proceeding that the local municipality has in the context of this surveillance recorded not only public areas or municipality owned property but also entrances and windows of the surrounding local privately owned buildings located in this square. This constituted in the opinion of the IC an invasion of privacy of the individuals who either resided in these buildings or were occasional or incidental visitors of this public area and have been consequently exposed to unavoidable and constant video surveillance. It was concluded that the video surveillance should not be used as a tool for the maintenance of law and order since specific services are entrusted with this task. In addition this excuse could serve as clarification for overall and constant video surveillance of all public areas which is not acceptable or justifiable. Therefore the IC concluded that the video surveillance in this case was illegal and that the local municipality might eventually be allowed to conduct the direct and focused video surveillance exclusively over the municipality owned defibrillator which is located on the facade of the post building in this square, for the purpose of assurance of the safety of people (for whom this device has been installed) and its property (for ex. from theft or destruction). The IC consequently ordered the local municipality to stop conducting of the video surveillance in this square and to irreversibly delete all recordings of the camera in question.

3. Inadequate security of personal data in on line application

The IC initiated an inspection proceeding against a supervisory authority due to the lack of security and accuracy of the data contained in the publicly accessible online application *Supervizor*. It has been established that it is possible to search for individuals in the *Supervizor* database only by entering the name and surname of a shareholder of a specific company in Google search engine, and that it is hence possible to even find data on a company and its shareholders that has not existed since 2013.

The IC found that the data, published in the application *Supervizor*, indeed originated from the Business Register and were, according to the Court Register of Legal Entities Act, public data. However, the law stipulated that the search through the data related to natural persons had to be limited in a way that it was only possible to search for natural persons in the Court Register by entering a combination of a name,

surname and citizen identification number or a combination of name, surname and tax number or a combination of a name, surname and address. When the data were transferred from the Court Register to the *Supervizor* application the supervisory authority should have established the same regime of data security and disclosure. Since that was not the case, and the data in *Supervizor* application were not protected properly, all internet users could find the information whether a certain individual was the founder, stakeholder, representative or a member of supervisory board of a certain legal entity, simply by entering the name and surname in a search engine. The supervisory authority could have prevented that by limiting search engine's access to the data with the so called robots.txt files or by only showing the data in non-machine readable format (such as a picture). The IC instructed the supervisory authority to ensure that the data in the *Supervizor* application are adequately protected so as to disable access of search engines to the names and surnames.

4. Unlawful collection of personal data of the holders of tickets

The IC conducted and inspection proceeding against a of public train service provider who was processing the passengers' location data (time, date, track and number of the train taken) without their knowledge. It has been established that the train service provider offered a number of different tickets, among them also contactless chip cards, where the chip contained the name and surname of the card holder and the data on the ticket – the type, validity, track, type and class of the train. The train service provider was collecting only location data of the holders of pre-paid tickets and holders of tickets with special discount for the railway employees. Location data were read and entered into the database when the ticket was read at the terminal on the train, essentially to check validity of the ticket

The IC held that there was no legal basis for the train service provider to process location data, since the passengers were not informed about it and did not consent to it. Processing of location data was neither necessary for performance of the contract between the train service provider and the passenger since the pre-paid ticket offered an unlimited number of travels in Slovenia or on a certain track. In such case the location of the passenger is irrelevant in terms of the contract. Processing constitutes a violation of the passengers' information privacy since it is possible to follow his/her locations in an extended time period. The train service provider was also conducting a public service as the only provider of transport in railway traffic; that is why it should be even more limited regarding the collection of passengers' data, since they did not have a choice of another provider if they wished to travel by train. Location data was also not vital for reporting on the quality of services, statistics, or as evidence of liability in train delays. The provider was ordered to delete the collected location data and to stop further collection and processing.

5. Collection and publication of personal data in the Supervizor application

The IC initiated an inspection procedure against a supervisory authority regarding the lawfulness of data collection and publication in the context of the application Supervizor which enabled online publication of the data on payment transactions of the budget users. It concerned individuals who have received payments from public sector entities, on the basis of a contract for copyrighted work or work contract. The data base was established in 2011 and has been updated daily with the data from the Public Payments Administration of Slovenia.

It has been established that the supervisory authority may, on the basis of the Integrity and Prevention of Corruption Act, collect the personal data that is necessary for the performance of its lawful duties. Until 4. 3. 2015, when the authority began its systemic investigation, there was no legal basis processing of the above mentioned data on the recipients of payments, which meant that the data on recipients' bank accounts acquired from 2011 on were in fact processed unlawfully up to the above date. The IC also held that the supervisory authority was following a lawful purpose of ensuring transparency of the work of public sector and that it has ensured proportionality of the published data – only the public information was disclosed, namely the data that referred to the payments of the public sector bodies which was related to the use of public funds. Publication was limited timewise as well as in terms of the payment – only the

recipients that have received over 150.000 Euros of payments in 10 years were disclosed, which represented less than 1 percent of all the recipients of payments from public sector entities.
The IC also found that the supervisory authority has been, since 2011, unlawfully receiving from the Public Payments Administration of Slovenia data on bank accounts of individuals who have received other types of payments, not related to contracts for copyrighted work or work contracts. The authority was ordered to delete from its data base the bank account numbers of all such individuals, since their data was not necessary in a specific procedure of the supervisory authority, and was acquired in bulk. The IC concluded that the supervisory authority violated the right to data protection of a large number of individuals whose data were included in the database. In case of most of them the supervisory authority did not have the competence to oversee their actions.

UKRAINE

CONTRIBUTION

for the 33rd T-PD meeting

The control functions of compliance with the legislation on personal data protection in Ukraine are assigned to the Ukrainian Parliament Commissioner for Human Rights (hereinafter referred to as the «Commissioner»). This approach ensures implementation of the international standards regarding independence of the national supervisory authority responsible for enforcement of legislation on personal data protection.

As it was noted in the Sixth Progress Report of the European Commission on the Implementation by Ukraine of the Action Plan on Visa Liberalisation (December 2015), the Ukrainian authorities have been satisfactorily implementing the law on protection of personal data and the independent data supervisory authority operates efficiently.

With the purpose of monitoring the observance of legislation on personal data protection in 2015-2016, employees of the Department for Personal Data Protection of the Secretariat of the Commissioner carried out numerous scheduled and unscheduled inspections of personal data controllers (bodies of state power, enterprises, other institutions and organizations, irrespective of the form of their ownership).

Employees of the Department for personal data protection carried out inspections in following spheres of public relations: social and medical services, housing and communal services, telecommunications and other consumer services, military, migration, law enforcement, education and so on. Inspections were also carried out in orphanages, boarding institutions for children, geriatric boarding institutions, nursing homes for elderly and disabled etc. It is also planned to conduct inspections of insurance and collection companies, providers of transport and travel services, as well as retail trade companies in 2016.

It should be noted that the number of inspections increase every year. 62 inspections were held in 2015, while in 2014 it was 53. 40 inspections have been conducted in 2016 as of June 15.

The Secretariat of the Commissioner constantly receives numerous complaints from natural persons with regards to violation of their right for protection of personal data. One of the most pressing issues that appeared in 2015 and should be given special attention in the future is compliance with the personal data protection legislation on the Internet.

Law of Ukraine «On Personal Data Protection» meets the requirements of international legislation on personal data protection. However, practical application of its provisions has shown the necessity of improvement of the legislation regulating this sphere, in particular by amendments to the Law.

With assistance of the Council of Europe Office in Ukraine the working group for preparation of amendments to the Law of Ukraine «On Personal Data Protection» was set up in the Verkhovna Rada Committee on Human Rights, National Minorities and Interethnic Relations.

During the first meeting of the working group in April 2016 the Concept on Improvement of the legislation on protection of personal data was presented. The aforementioned Concept was developed by the employees of the Department for personal data protection of the Secretariat of the Commissioner.

Experts of the Council of Europe, Ms. Marie Georges and Mr. Graham Sutton, took part in the working group meeting and supported the Concept. The experts of the Council of Europe also supported the aspiration of Ukraine to develop an effective system of protection of personal data, and also expressed their remarks and proposals to the Concept on Improvement of the legislation on protection of personal data. The importance of application of the newest European legislation tendencies, namely modernized the Convention for the Protection of Individuals with regards to the Automatic Processing of Personal Data. The Regulation 2016/679 and Directive 2016/680 of the European Parliament and the Council have recently been adopted, in the process of amending the Law of Ukraine «On Personal Data Protection».

In this regard on May 23rd-24th, 2016, experts of the Council of Europe Ms. Marie Georges and Mr. Hansjürgen Garstka, presented recent trends in the development of general legal regulations of personal data protection in Europe to the employees of the Secretariat of the Commissioner during the training «Tendencies of development of European legal regulation on personal data protection».

Educational work on the practical application of the personal data protection legislation with purpose of raising public awareness on the matter was among the priorities of the Commissioner in 2015-2016.

A series of regional one-day sectorial trainings on personal data protection for advocates and representatives of healthcare and law enforcement were held by the Department of Personal Data Protection of the Secretariat of the Commissioner in cooperation with the Council of Europe Office in Ukraine, within the framework of the Council of Europe and the European Union Joint Programme «Strengthening Information Society in Ukraine» (at present the Programme is finished).

Within the framework of the aforementioned Programme «Strengthening Information Society in Ukraine», in cooperation with the Council of Europe Office in Ukraine and with assistance of the Ukrainian Catholic University and the Secretariat of the Commissioner, the project «School of Personal Data Protection» has also been launched, which is a three-day training course for target groups. Representatives of telecommunication companies, banks and military have already passed the course.

Cooperation with the European Union and the Council of Europe has continued in 2016 within the framework of another project – «Strengthening the Implementation of European Human Rights Standards in Ukraine». In particular, within the framework of this project the «School of Personal Data Protection» for healthcare representatives and for legal departments of central bodies of executive power has been organized. During a three-day course people responsible for the organization of the protection of personal data, and other persons involved in processing of personal data, attend lectures held by employees of the Department for Personal Data Protection of the Commissioner, and by European and Ukrainian experts in the sphere of personal data protection. During colloquiums participants may test the knowledge they have gained.

UKRAINE - MEDIATRICE DE L'UKRAINE

Le respect du droit à la protection des données à caractère personnel
(La version abrégée)

Toute personne a le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Cette disposition est fixée dans l'article 8 de la Convention européenne des droits de l'homme et garantie par l'article 32 de la Constitution de l'Ukraine.

Le mécanisme de protection du droit à la vie privée, y compris la protection des données à caractère personnel est déterminé par la loi de l'Ukraine «Sur la protection des données à caractère personnel".

Dans le sixième rapport final de la Commission européenne sur la mise en œuvre par l'Ukraine du Plan d'action sur la libéralisation du régime de visa il a été noté que l'Ukraine accomplit de manière satisfaisante la loi "sur la protection des données à caractère personnel» et assure le fonctionnement efficace de l'autorité pour le contrôle indépendant de la protection des données à caractère personnel.

En 2015, la Médiatrice Ukrainienne Parlementaire aux droits de l'homme (ci-après – la Médiatrice) a reçu 638 plaintes des citoyens et des personnes morales concernant la réalisation du droit à la protection des données à caractère personnel. Essentiellement, les plaintes portaient sur le traitement des données à caractère personnel dans le secteur financier, le secteur du logement et des services communaux et l'Internet.

Pour mettre en œuvre les charges du contrôle imposées à la Médiatrice sur le respect de la législation sur la protection des données à caractère personnel, au cours de 2015 employés du Département de la protection des données à caractère personnel du Secrétariat de la Médiatrice ont effectué des inspections des autorités publiques, des gouvernements locaux et des entreprises, des institutions et des organisations de toutes les formes de propriété. En 2015 62 inspections planifiées et non planifiées des maîtres du fichier ont été conduites. À la suite des inspections les prescriptions ont été envoyées aux entités de vérification pour éliminer les violations de la législation sur la protection des données à caractère personnel identifiées lors de l'inspection qui ont été entièrement fait par le titulaire et/ou maître du fichier des données à caractère personnel.

En outre, au cours de 2015, dans le cadre des actions du contrôle prévues et imprévues sur le respect de la législation sur la protection des données à caractère personnel employés du Département de la protection des données à caractère personnel du Secrétariat de la Médiatrice a rédigé 3 procès-verbaux concernant engagement de la responsabilité administrative. Après avoir examiné les cas d'infractions administratives, soumis à la cour, deux délinquants ont été reconnus coupables et ont été sujets à la responsabilité administrative.

Les employés du Département de la protection des données à caractère personnel du Secrétariat de la Médiatrice conduisent régulièrement les cours éducatifs pour les groupes cibles professionnels sur l'application pratique de la législation sur la protection des données à caractère personnel.

Donc, avec le soutien du Bureau du Conseil de l'Europe en Ukraine dans le cadre d'un programme commun de l'Union européenne et le Conseil de l'Europe "Renforcement de la société d'information en Ukraine" le Secrétariat de la Médiatrice a organisé une série de séminaires sur les questions relatives à l'application de la loi sur la protection des données à caractère personnel. Avec le soutien du Bureau du Conseil de l'Europe en Ukraine le projet "Une école de la protection des données à caractère personnel" se réalise, qui est un cours de trois jours pour les groupes cibles.

Sur la base des appels des organes centraux exécutifs, des citoyens et de son propre arbitre, le Département de la protection des données à caractère personnel du Secrétariat de la Médiatrice a effectué en continu une analyse des règlements et leurs projets concernant le traitement des données à caractère personnel.

En particulier, au cours de la dernière année environ 34 projets d'actes juridiques ont été creusés, y compris les 15 projets de loi, cinq projets de règlements du Cabinet des ministres de l'Ukraine, 14 projets d'actes juridiques des organes de l'Etat. Presque tous les projets d'actes normatifs ont eu besoin de la révision afin de les mettre en conformité avec l'article 32 de la Constitution de l'Ukraine et de la loi de l'Ukraine «Sur la protection des données à caractère personnel". Dans la plupart des cas, les observations de la Médiatrice ont été prises en compte.

Projet de loi de l'Ukraine "Sur les modifications à l'article 25 de la loi de l'Ukraine "Sur la protection des données à caractère personnel" (№ 2959 du 26.05.2015) a proposé les modifications qui permettraient le traitement des données à caractère personnel sans l'application des dispositions de la loi

de l'Ukraine "Sur la protection des données à caractère personnel" par les personnes physiques et morales afin de "faciliter" pour certains des autorités de l'Etat la mise en œuvre des mesures nécessaires pour protéger la sécurité d'Etat et public, les intérêts financiers de l'Etat et de lutter contre les infractions pénales".

En fait par telles modifications il a été proposé de porter les activités des certains autorités publiques en dehors du champ d'application de la réglementation de la loi de l'Ukraine «Sur la protection des données à caractère personnel". Cette disposition créerait une menace du contrôle absolu des organes d'application de la loi sur tous les aspects de la vie privée des citoyens de l'Ukraine, contrairement aux normes reconnues des droits de l'homme et la protection des données à caractère personnel. Suite aux observations de la Médiatrice le Comité de la Verkhovna Rada de l'Ukraine sur l'information et de la communication a recommandé Verkhovna Rada de l'Ukraine de rejeter le projet de loi.

Il convient de noter que l'analyse des actes juridiques normatifs a constaté une pratique généralisée de la compréhension fausse et l'application du principe de légalité du traitement des données à caractère personnel par les entités de l'initiative législative, du fait que la mise en œuvre de ce principe dans le projet de loi est limitée seulement par la définition formelle du droit de l'organe d'Etat de traiter les données à caractère personnel. Cependant, le principe de la légalité du traitement (de distribution) des données à caractère personnel ne se limite pas au fait que le droit d'accès aux données à caractère personnel doit être défini dans la loi.

Ainsi, la Cour européenne des droits de l'homme dans ses décisions reconnaissent un atteint à la vie privée comme légitime, s'il est envisagé par les dispositions du droit national qui est un signe de la «qualité de la loi». Autrement dit, les lois doivent être «accessible aux parties concernées et prévisible sur les conséquences de leurs applications". La norme est «prévisible» si elle est formulée avec suffisamment de précision qui permet à quiconque, qui a besoin, de concilier son comportement.

Dans le même temps, il y a une pratique assez courante lorsque la loi qui autorise à traiter les données à caractère personnel, ne contient pas des dispositions relatives aux fins de leur utilisation, composition des données à caractère personnel, leur conservation à long terme, les droits d'accès de tiers, de sorte que tous les aspects du traitement des données à caractère personnel qui conformément à loi de l'Ukraine «Sur la protection des données à caractère personnel» devrait être défini par la loi. Même lorsque les législateurs autorisent l'organe d'Etat à déterminer soi-même la procédure spécifique pour le traitement des données à caractère personnel, la loi ne définit pas «orientations» claires sur la justification de l'atteint à la vie privée. Ce facteur clé devrait être l'objectif du traitement des données à caractère personnel, qui doivent être claires et compréhensibles. À cet égard, il convient de souligner que les modifications apportées à la législation (y compris le Code du budget de l'Ukraine et la loi de l'Ukraine «Sur les banques et les activités bancaires») en termes de l'octroi d'accès de l'organe central du pouvoir exécutif, qui prévoit la formation de la politique financière du gouvernement (Ministère des Finances de l'Ukraine), à l'information sur les individus, ce qui inclut le secret bancaire et d'autres données à caractère personnel est incompatible avec les dispositions de la Constitution de l'Ukraine et de la loi de l'Ukraine "Sur la protection des données à caractère personnel".

En 2015, il y avait un problème actuel concernant l'utilisation abusive par les titulaires des normes de la législation sur la protection des données à caractère personnel, en particulier concernant les raisons du traitement des données à caractère personnel ce qui fait que les conditions préalables sont créées pour violation des droits constitutionnels, par exemple le droit à la protection sociale.

En particulier, il y avait de nombreuses appels des citoyens de l'Ukraine avec une demande de protéger leurs droits en cas de nomination refusée de subventions au logement en ne fournissant pas leur consentement au traitement des données à caractère personnel.

Cela est dû au fait que le modèle de la déclaration pour la nomination des aides au logement approuvés par un arrêté du Cabinet des Ministres de l'Ukraine le 28 Février, 2015 № 106 «Sur l'amélioration de la procédure d'octroi des subventions au logement" contient la clause concernant l'octroi par le demandeur et les membres de sa famille de son consentement concernant le traitement des données à caractère personnel sur la famille, le revenu familial, les biens qui sont nécessaires pour la nomination des subventions au logement et la promulgation de l'information sur sa nomination.

Ainsi, en signant une déclaration, la personne donne son consentement au traitement des données à caractère personnel. Toutefois, l'article 5 de la loi de l'Ukraine «Sur les services de logement et communaux" prevoit que l'organe exécutif central qui met en œuvre la politique de l'Etat dans le domaine de la protection sociale, organise le travail sur la nomination et l'octroi de subventions. Ainsi, le traitement des données à caractère personnel dans la nomination des subventions au logement est effectué conformément au paragraphe 2 de l'article 11 de la loi de l'Ukraine «Sur la protection des données à

caractère personnel". Dans telles circonstances, l'inclusion du point de déclaration à fournir par demandeur et membres de la famille le consentement au traitement des données à caractère personnel est totalement injustifiée d'un point de vue juridique.

Ainsi, il y a la situation où la mise en œuvre du droit d'obtenir un logement subventionné est rendue dépendante de l'octroi de tel consentement, qui viole garanti par l'article 46 de la Constitution de l'Ukraine droit à la protection sociale. En réponse aux appels répétés de la Médiatrice au Ministère de la politique sociale de l'Ukraine il a noté que l'absence du consentement des requérantes au traitement des données à caractère personnel empêche nomination de subventions au logement pour eux, et donc le problème reste indécis.

Il convient également de noter que le public continue d'envoyer des plaintes au sujet de telles demandes illégales de sociétés de services publics comme l'octroi des copies des passeports, numéro d'enregistrement de la carte de personne assujettie à l'impôt, les documents attributifs pour le logement en concluant le contrat.

Collecter et conserver des copies des documents requis pour les contrats avec les consommateurs, l'entreprise concernée peut seulement sur la base du consentement volontaire des consommateurs. Par exemple, un employé du fabricant de services publics peut proposer aux consommateurs de fournir des copies des documents pour l'accélération et la facilitation de l'émission du contrat. Dans ce cas, le consommateur aura la possibilité de transférer des copies de documents.

Aussi à la fin de 2015 à travers les médias l'information était largement diffusée sur la collecte d'information trop détaillée par les commissariats militaires concernant les futures recrues et leurs familles. En particulier, les commissariats militaires a exigé les futures recrues de remplir la soi-disante «Attestation sur la famille de recrue".

Dans le mentionné ci-dessus "Attestation sur la famille de recrue" il était nécessaire d'indiquer les données à caractère personnel des recrues et leurs parents qui sont classés comme des données à caractère personnel "sensibles". Ces données comprennent, notamment, la nationalité, l'état de santé, les croyances religieuses. Ce sont les informations sur eux-mêmes, leurs parents et d'autres parents qui ont été demandés par les commissariats militaires de recrues. Il convient de noter que le traitement de ces données est interdit en vertu de la Convention sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (article 6) et la loi de l'Ukraine «Sur la protection des données à caractère personnel" (article 7) et, à titre exceptionnel, est autorisé seulement dans les cas clairement définis par la loi.

Il était également incompréhensible le but de recueillir d'autres données à caractère personnel, sur la propriété de la famille de recrue, lieu de travail, des informations sur les affaires judiciaires, qui a été siégé par des parents des recrues, la présence des animaux domestiques etc.

Pour remédier à cette situation, la Médiatrice s'est adressée au Ministère de la Défense de l'Ukraine avec une soumission, en vertu de laquelle les mesures sont prises pour éliminer les violations du droit constitutionnel à la vie privée, qui est confirmé par la lettre du Ministère de la Défense de l'Ukraine. Ainsi, "Attestations sur la famille des recrues» ont été retirées des dossiers personnels des recrues et détruites en temps voulu. Aussi le texte de "l'Attestation sur la famille des recrues" a été mis en conformité avec la loi sur la protection des données à caractère personnel.

Le respect de la protection des données à caractère personnel sur Internet sont les problèmes les plus douloureux de la protection des données à caractère personnel qui est apparu sensible en 2015 et auxquelles une attention particulière doit être prêter à l'avenir .

En particulier, nous avons reçu de nombreuses plaintes de citoyens sur la distribution illégale de leurs données à caractère personnel sur certains sites Web. Malheureusement, il n'y a pas de mécanisme législatif pour bloquer l'accès des utilisateurs à toute ressource Internet. À cet égard, il existe un besoin urgent d'apporter les modifications appropriées à la législation qui pourraient affecter efficacement le fonctionnement de ces sites qui enfreignent la loi pour la protection des données à caractère personnel.

L'un des plus commun est une violation du droit d'accéder à leurs données à caractère personnel. Les départements des fonds de pension ont refusé de fournir des copies des affaires et de documents de retraite liés aux pensions, les employeurs - les copies des documents relatifs à la mise en œuvre des contrats de travail, les établissement de soins - les copies des dossiers médicaux. En outre, la Médiatrice reçoit des plaintes pour violation du droit d'accéder aux données personnelles des établissement d'éducation, du logement et des services communaux. Dans certains cas, leur refus de fournir un tel accès à des données à caractère personnel le titulaire justifie que l'information demandée est contenue dans les documents pour l'usage officiel, sans référence à des dispositions spécifiques de la législation qui limitent l'accès de personne à l'information.

Refus d'accès à l'information sur eux-mêmes, sans référence à une loi qui contient la règle directe sur la limitation du droit d'obtenir de telles informations est contraire à la loi de l'Ukraine «Sur la protection des données à caractère personnel" et une violation de l'article 32 de la Constitution de l'Ukraine, selon laquelle chaque citoyen a le droit de faire connaissance avec les informations sur eux-mêmes dans les organes du pouvoir d'Etat, les collectivités locales, les institutions et les organisations qui n'est pas étatique ou un autre secret protégé par la loi .

URUGUAY

"Since the last meeting, Uruguay has been advancing in the path to educate individuals on the importance of data protection.

The URCDP has been a promoter of reaching controllers and public authorities throughout education, rather than by imposing sanctions.

In that spirit, it has hosted four events with participation of civil society, private and public sector to discuss specific issues regarding children, big data, amongst others. Results on the discussions were later posted on the Unit´s webpage.

The URCDP also organized, as every year, the "Tus Datos Valen" contest aimed at children, with support of the Public Schooling System, the Official Gazzette, and the Ceibal Foundation. The objective of the contest in the 2015 version was to create a screenplay regarding the protection of personal data and produce a short clip. Various schools from around the country presented their work, two winners were selected, and a small number of mentions were awarded.

From the international point of view, the Unit has been engaged with other DPAs in a number of important activities to promote data protection in Latin America.

Finally, in the regulation field, a recent law simplified the process of requesting the close down of databases to the Courts, thus improving the Unit´s sanctionatory powers. It has also clarified some doubts on the interpretation of the applicability of data protection to some labour documents, stating that the latter are in compliance with data protection law. This will bring greater certainty to the relations between employers, employees and authorities."

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

2015 will be remembered as the year the EU seized an historic opportunity. The General Data Protection Regulation (GDPR) is one of the EU's greatest achievements in recent years. It is a set of data protection rules for the digital age, an ambitious and forward-thinking agreement of which the EU can be proud.

The EDPS mandate and our EDPS Strategy 2015-2019 are designed to address the current period of unprecedented change and political importance for data protection and privacy, both in the EU and globally, and the EDPS intends to ensure that the EU remains at the forefront of the debate. Our Strategy of leading by example, which was published in March 2015, will be pursued further in 2016, as we look to build on the achievements of 2015 and develop innovative solutions to the data protection challenges which face us.

EDPS Strategy 2015-2019

At the beginning of his mandate in 2015, the new EDPS finalised a strategy for the coming five years. His aim was to turn his vision of an EU that leads by example in the debate on data protection and privacy into reality and to identify innovative solutions quickly. This Strategy provided the basis for our work throughout 2015.

The Strategy identifies three strategic objectives and 10 actions to achieve our aims:

1 Data protection goes digital

(1) Promoting technologies to enhance privacy and data protection;

(2) Identifying cross-disciplinary policy solutions;

(3) Increasing transparency, user control and accountability in big data processing.

2 Forging global partnerships

(4) Developing an ethical dimension to data protection;

(5) Speaking with a single EU voice in the international arena;

(6) Mainstreaming data protection into international policies.

3 Opening a new chapter for EU data protection

(7) Adopting and implementing up-to-date data protection rules;

(8) Increasing accountability of EU bodies collecting, using and storing personal information;

(9) Facilitating responsible and informed policymaking;

(10) Promoting a mature conversation on security and privacy

Overview of Activities

Since the last Plenary meeting of the Committee of Convention 108, we have continued our work along five main themes. We also provided recommendations on the EU data protection reform and made contributions to several high profile court cases which resulted in important rulings.

Borders

Terrorism and migration rated high on the EU agenda in 2015. EDPS work on borders has therefore started to take on increasing importance. We ensured that data protection and privacy remain primary concerns, both by providing advice on new legislation to combat terrorism and by continuing to effectively supervise the large-scale IT systems used by the EU to process visa, asylum and other similar requests.

Activities of particular note included:

- Supervision of the PeDRA project at Frontex, a project designed to better manage information related to people smuggling and human trafficking
- The second EDPS Opinion on the Personal Name Record (PNR) Directive
- Supervision of an assessment carried out by eu-LISA on the performance of Multi-Spectrum Imaging (MSI) devices, for the scanning of fingerprints
- Inspections of the Visa Information System (VIS) and the Schengen Information System (SIS) to check the security and operational management of these databases

Security

With continued developments in technology, work on security, particularly as it relates to the day-to-day work of the EU institutions and bodies, remained a strong focus for the EDPS. During 2015 we issued Guidelines on the use of electronic communications and mobile devices in the workplace, whilst also working with EU institutions and bodies and their Data Protection Officers (DPOs) to ensure the implementation of effective security measures such as encryption and to deal with data breaches.

We also issued an Opinion on intrusive surveillance technology in which we highlighted the risks posed by the unregulated and growing market for the sale, distribution and (dual) use of spyware. We emphasised the need to do more to effectively monitor the market and called on legislators to look for safeguards which embed privacy by design in technology and ensure that it is secure.

Responding to new challenges

2015 presented many new challenges and much of our work focused on how to respond to them. We monitored new technologies, issuing an Opinion on big data, and worked with other EU institutions and bodies to address the data protection concerns raised by a number of EU initiatives. These included:

- Working with the Commission to develop a Data Protection Impact Assessment (DPIA) framework and to identify Best Available Techniques (BATs) for the operation of smart meters
- Following developments related to the Commission's platform for cooperative intelligent transport systems (C ITS)

We also launched two new projects, the Ethics Advisory Group and our mobile app on the General Data Protection Regulation (GDPR), and continued to develop the Internet Privacy Engineering Network (IPEN), all aimed at promoting a proactive approach to data protection in the EU and globally.

Global dimension

In accordance with the vision outlined in the EDPS Strategy 2015-2019, we have been working hard to develop the global dimension of our work. We have contributed fully to European and international fora and actively monitored and provided advice on international agreements with an impact on data protection.

This approach was particularly evident in our response to the decision by the EU Court of Justice to invalidate the Commission's Safe Harbour decision. We worked with fellow data protection authorities in the WP29 to analyse the consequences of this ruling and with DPOs in the EU institutions to determine its impact on their activities.

In addition to our work with the WP29, we continued to develop effective working relationships with international organisations, including the Council of Europe, and contributed significantly to a range of international conferences and events, including the European Conference of Data Protection Authorities and the International Conference of Data Protection and Privacy Commissioners.

The EDPS is also responsible for providing the Secretariat for the supervision coordination groups of several large-scale IT systems which include vast amounts of data. In 2015, we organised two meetings for each of the coordinated supervision groups, ensuring that the meetings of all groups took place one after the other, so that consistent and horizontal supervision policies could be implemented where possible.

On the ground

We have continued to supervise and provide advice to the EU institutions, carrying out inspections, issuing prior check Opinions and developing our relationships with the DPOs who are responsible for ensuring compliance with data protection law within their respective EU institutions. Our work in the latter half of 2015 included:

- The development of a checklist to provide practical guidance to EU institutions on the implementation of whistleblowing procedures
- Inspections to ensure that investigations in the EU institutions related to fraud, anti-harassment and due diligence respect data protection rules
- Working with the Commission to develop their Cloud Computing Strategy
- Strengthening relations with DPOs through a more interactive and hands-on approach to our biannual meetings

GDPR: EDPS recommendations for reform

After almost four years of negotiation, the General Data Protection Regulation (GDPR) was agreed in December 2015. The GDPR will replace the current Directive 95/46/EC.

Ever since the European Commission presented the original legislative proposal in January 2012, the Reform has been the subject of intense debate. The EDPS followed developments throughout the legislative process, providing advice to the EU co-legislators (the European Parliament and the Council) at various stages.

On 27 July 2015, we produced our recommendations on the proposed legislation, for use by the EU co-legislators when negotiating the final text of the GDPR. We also launched a mobile app, allowing tablets and smartphones to be used to easily compare the texts proposed by the Commission, the European Parliament and the Council, alongside the recommendations from the EDPS.

The proposed new rules will affect all individuals in the EU, all organisations in the EU who process personal data and organisations outside the EU who offer goods or services to the EU or monitor the behaviour of individuals in the EU. It represents an opportunity for Europe to lead by example on a global level, setting the standard for the rest of the world to follow.

Court Matters

The right of the EDPS to intervene in actions before the court was recognised by the Court of Justice of the EU (CJEU) in the PNR cases (Cases C-317/04 and C-318/04, orders of 17 March 2005). The court based the right to intervene on the second subparagraph of Article 41(2) of Regulation (EC) No 45/2001 according to which the Supervisor is 'responsible for advising Community institutions and bodies on all matters concerning the processing of personal data'. This advisory task does not only cover the processing of personal data by those institutions or organs. The Court interpreted the powers conferred on the EDPS by Article 47 of the Regulation in light of the purposes of Article 41.

In 2015, the EDPS was involved in a range of high-profile cases which resulted in important rulings. These rulings have both helped us to more clearly define data protection law and to ensure that the fundamental right to privacy and data protection is fully respected.

In July 2015, the CJEU ruled on two cases related to transparency and data protection: Case T-115/13, Dennekamp v. European Parliament and Case V-615/13, ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA). The EDPS intervened in both of these.

The cases gave an insight into the arguments which meet the criteria of necessity and proportionality and the arguments that do not, allowing us to further define and understand the relationship between data protection and transparency.

On 24 March 2015, the EDPS pleaded before the General Court of the European Union in Case T-343/13 concerning the handling of petitions by the European Parliament. The plaintiff accused the Parliament of having unlawfully published his personal data on the European Parliament website when handling his petition.

The Court's judgment, published on 3 December 2015, followed the same legal reasoning used by the EDPS. However, contrary to our conclusions, it judged that the information provided by the Parliament to the petitioner when requesting consent for the publication of his personal data was appropriate and that the petitioner's consent was therefore given. The case was consequently dismissed.

Also on 24 March 2015, the EDPS intervened before the Court of Justice of the European Union at the hearing of Case T-343/13 Maximillian Schrems v Data Protection Commissioner, concerning the Safe Harbour agreement. The EDPS is not admitted to intervene in preliminary ruling procedures and was therefore not a party to the case. The Court is, however, entitled to ask the EDPS to submit observations on the case in its role as advisor to the European institutions on data protection.

The Court ruled the Safe Harbour agreement invalid in October 2015. We continue to work with our colleagues in the WP29 to address the repercussions of the ruling.

INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC)

Council of Europe T-PD 33rd Plenary meeting (Strasbourg, 29 June -1 July 2016)

CONTRIBUTION : Major developments in the data protection field

1. Background

In February 2015 the ICRC adopted the ICRC Rules on Personal Data Protection.

Available here: https://www.icrc.org/en/publication/4261

2. Institutional/Compliance/Remedy

Q4 2015 The ICRC set up a Data Protection Office. More information, including role, tasks, and responsibilities can be found here: https://www.icrc.org/en/document/icrc-data-protection-office

Q1 2016 The ICRC Assembly amended the ICRC Statutes to set up the ICRC Data Protection Commission as a new Governing Body. More information, including Members' profiles, role, tasks, responsibilities and ICRC Statutes can be found here: https://www.icrc.org/en/document/icrc-data-protection-independent-control-commission

3. Information/Communication

On the occasion of the Data Protection Day, the ICRC published on its website dedicated pages covering Data Protection at the ICRC. The pages can be found here: https://www.icrc.org/en/document/data-protection

4. External Engagements/Policy

ICRC/EDPS Workshop on Data Protection in International Organisations

On 5 February 2016 the ICRC Data Protection Office co-organised with the European Data Protection Supervisor, and hosted in Geneva the Fifth Workshop on Data Protection in International Organisations.

More information is available from the links below:

- https://www.icrc.org/en/event/5th-workshop-data-protection-within-international-organisations
- https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Intorg

ICRC/Brussels Privacy Hub: Data Protection and Humanitarian Action working series

In June 2015 the ICRC Data Protection Office and the Brussels Privacy Hub launched a working series on Data Protection and Humanitarian Action, aimed at analyzing and providing guidance on the application of Data Protection requirements in Humanitarian Action, particularly when new technologies are involved.

The workshops bring together Humanitarian Organisations, Data Protection Authorities, experts on the specific technologies involved, and private companies active in the use of such technologies to ensure the necessary expertise is available.

The working series is also aimed at feeding into the work launched by the International Conference of Privacy and Data Protection Commissioners under its 2015 Resolution on Privacy and International Humanitarian Action.

As part of this working series, the ICRC and the Brussels Privacy Hub held four workshops on the following topics:

- Data analytics
- Drones/UAVs
- Biometric data
- Cash transfer programming

Two additional workshops are foreseen before the end of 2016. The outcome of these workshops will be published in the course of 2017.

Additional information is available from the following links:

- https://www.icrc.org/en/document/data-protection-humanitarian-action
- http://www.brusselsprivacyhub.org/project.php