COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 26 June / juin 2017

T-PD(2017)08Mos

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

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

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

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

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

TABLE OF CONTENTS / TABLE DES MATIERES

ALBANIA / ALBANIE

Activities in implementation of the law on personal data protection

MAJOR DEVELOPMENTS IN DATA PROTECTION FIELD
"June 2016-June 2017"

INFORMATION AND DATA PROTECTION COMMISSIONER OF ALBANIA

- *Adoption of by-laws*

Instruction no. 44/2016 of the Commissioner *"On the conditions, processing criteria and the time of retention of personal data in law enforcement no. 60/2016" obligation set up by law "On the protection of whistleblowers"*. **Joint instruction no. 515, dated 07.09.2016** of the Minister of Internal Affairs and the Commissioner, *"On the processing of personal data by Border Guards"* pursuant to law no. 71/2016 "*On border control".* **Instruction no. 45, dated 31.10.2016** "*On an amendment to the Instruction no. 3/2010 "On the processing of personal data in the video surveillance system in buildings and other premises".* **Instruction no. 46, dated 28.03.2017** *"On determining the security level for the processing of personal data through security systems, pursuant to law no. 19/2016 "On additional public safety measures".*
Instruction adopted by the Commissioner "On determining the controllers obliged to notify the Commissioner's Office on processing of personal data, for which they are responsible, for the first time or when required following the change of processing notification".
Instruction adopted by the Commissioner "On the processing of sensitive data and obtaining authorizations".

- *Rendering opinions on draft/legal acts and by-laws*

The Commissioner's Office continues to encourage public and private entities, to submit any legal and sub-legal drafts, legal documents, agreements, etc, relating to the field of personal data protection for legal opinion:

Draft law "On Social Services in the Republic of Albania" submitted by the Ministry of Social Welfare and Youth.
Draft law "On some addendums and amendments to law no. 9947 dated 07.07.2008 "On industrial property", as amended, submitted by the Ministry of Economic Development, Tourism, Trade and Entrepreneurship.
Draft law "On the protection of national minorities in the Republic of Albania", submitted by the Ministry of Foreign Affairs.
Draft law "On some addendums and amendments to law no. 10128, dated 11.05.2009 "On electronic commerce" as amended, submitted by the Minister of State for Innovation and Public Administration.
Draft law "On some addendums and amendments to law no. 9918, dated 19.05.2009 "On electronic communications in the Republic of Albania", as amended, submitted by the Minister of State for Innovation and Public Administration.
Draft decision "On the establishment of State Police Data Base for electronic management of fines (E-fines)", submitted by the Ministry of Internal Affairs.
Draft decision "On establishing of a state database in the national electronic health registration", submitted by the Minister of State for Relations with Parliament.
Draft decision "On establishing of a state database digital Archives of the Central Technical Archives of Construction" submitted by the Minister of State for Relations with Parliament.
Draft agreement between the Council of Ministers of the Republic of Albania and the Government of Georgia "On cooperation in the fight against crime", submitted by the Ministry of Internal Affairs.
Draft agreement on "Cooperation between Eurojust and Albania" submitted by the Ministry of Justice.
Project "On the installation of CCTV system in Civil Status Offices", submitted by the Ministry of Internal Affairs, as well as other drafts submitted by various Controllers.

- *Cooperation agreements*

IDP has also scored achievements in the inter-institutional relationship context. During this period, the Information and Data Protection Commissioner has signed several cooperation agreements.

Cooperation agreement with the Rectorate of the University of Tirana
Signed in December 2016, key component of this agreement is the establishment of the "Information and Privacy" Winter School, on continuous training of students in the field of privacy and the right to information.
Cooperation agreement with the National Chamber of Mediators
Signed in March 2017, crucial commitment of the parties is the implementation of highest standards with respect to the protection of privacy and personal data of citizens, whilst respecting the right to information regarding official documents, as well as joint organization of training or awareness related activities, joint application for projects and initiatives of interest and exchange of information in the context of research activities.
Cooperation agreement with the Information Authority on Former Sigurimi Files
Signed in April 2017, main purpose of this agreement is to guarantee and respect the fundamental human rights and freedoms, in particular in the area of the right to information and protection of personal data for all persons whose data has been stored and processed by Former "Sigurimi".

Cooperation with EUROJUST
As of May, negotiations have been triggered with EUROJUST regarding the agreement that is expected to be signed between the Republic of Albania and EUROJUST.
This agreement primarily aims to strengthen cooperation between EUROJUST and the Republic of Albania in the fight against serious crimes, particularly organized crime and terrorism. It integrates a special session for personal data processing, the rights of data subjects, and obligations of national authorities implementing law when using individual's personal data etc.
Parties have currently approved the draft which has been forwarded to EUROJUST's supervisor.

- **Notifications**

- ***Handling notifications and the registry of controllers/May 2015-May 2016***

During this period **197** controllers have notified the Commissioner, **8** of which being non-profit organizations, **15** public entities and **174** private entities, bringing the total number of notifications to 5311. Total number of registered entities in the public registry amounts to **5253.**

- ***Policies and the outcome of oversight***

The Office of the Commissioner applies its supervisory role through controls and inspections performed *ex-officio* or upon data subjects' complaints.

- *Handling of complaints*

Throughout this period, **82** complaints have been filed with the IDP Commissioner's Office, requests for information and data breaches claims regarding public or private controllers.

Complaints mainly referred to:

- Disclosure of personal data in the Media and on the official websites of controllers;
- Exercise of the data subjects' right to access, rectification/deletion of personal data;
- Processing of data without the consent of data subjects and without prior notification;
- Illegal disclosure of personal data

During this reporting period, a considerable number of complaints have been filed with Commissioner's Office via email at info@idp.al.

- *Administrative controls and inspections (ex-officio)*

In accordance with its supervisory policies, IDP has conducted a total of 131 sector-specific administrative controls and inspections with controllers exercising public and private functions. Such administrative controls and inspections focused on specific sectors such as:

- Banking sector
- Marketing sector (*call center*)
- Pre-university Education System (Public)
- Hotels -Tourism sector (Private)
- Employment sector (Private)

- Higher Education- Universities (Public and Private)
- Health sector
- Video surveillance
- Tourism agencies
- Public authorities
- Telecommunication (process of disclosure of personal data by the processors)
- Local government (online inspections and upon complaint)

The main purpose of the Commissioner's Office has been to verify the implementation of the legislation on the protection of personal data in specific sectors, point out issues and provide assistance in the framework of implementation and application of legal obligations.

- *Recommendations*

IDP Commissioner's Office has rendered a total of 103 Recommendations in aftermath of the administrative investigations, in cases where the infringements have not violated (or didn't have direct impact) the right to privacy of data subjects.
At the conclusion of the investigations conducted with Pre-university Education Sector and Tourism Agencies, based on the violations found during controls (infringements to Law no. 9887/2008 on Personal Data Protection as amended, and related by-laws), the Commissioner's Office has rendered Unifying Recommendations for the Ministry of Education and National Tourism Agency, as primary policy-making in the respective sector.

- *Administrative Sanctions (punitive fines)*

In cases of serious and repeated violations of law or failure to comply with its Recommendations and Orders, the Commissioner has imposed sanctions. A total of 38 decisions corresponding to 66 administrative sanctions with punitive fine.
Such sanctions refer mainly to infringements of legal obligation to inform data subjects, the obligation to implement security measures and confidentiality, the obligation to adopt the provisions regarding principles of personal data protection in contractual agreements with third parties, deadlines for data retention, the obligation to "Notify" the Commissioner's Office on the intended data processing, etc.
Such administrative sanctions imposed by the Commissioner's Office pursuant to the law, and in implementation of the principles of legitimacy, decision-making transparency and the right of the parties to be heard. Pursuant to Articles 87-88 of Law No. 44/2015 "Code of Administrative Procedures of the Republic of Albania", several hearings with controllers have been conducted before reaching the final decision of sanction with punitive fine.

- *International Transfer*

Special attention has been assigned to requests for authorization by the Commissioner for international transfer of data to countries that do not ensure adequate level of personal data protection, as set forth in the Commissioner's Decision no. 3, dated 20.11.2012 "On the determining of countries ensuring adequate level of personal data protection"
During this period 38 files have been examined and 12 decisions have been rendered. The Commissioner has examined such requests for authorization for international transfer of personal data without delay, due to administrative investigations conducted ex-officio or upon complaints and to the adoption of a new instruction and a new guidelines, thus facilitating and informing controllers throughout the process of filing a request for data transfer.

Public media and Communication

In the framework of the awareness raising campaign "Privacy and data security during the use of social networks by youth", the Commissioner's Office conducted from June till December 2016, 22 meetings with Secondary School of Elbasan, Vlora, Gjirokastra, Durrës, Lezha, Shkodra, Kukës, Fier, Berat, Lushnje, Pogradec, Korça, Tepelena, Përmet and Saranda. Safe use of internet and social networks were at the centre of these events as well as practical cases of data misuse and effective means to prevent privacy breaches. A questionnaire was distributed in order to identify the level of use of social networks. Following these seminars the IDP Commissioner's Office has prepared and published a comprehensive study.

The Commissioner's Office has held informative meetings with students and academic staff of Vlora University "Ismail Qemali", "Luigj Gurakuqi" of Shkodra, "Eqerem Çabej" of Gjirokastra, "Fan Noli" of Korça, "Aleksandër Moisiu" of Durrës and Saranda's branch of the Faculty of Economics of Tirana University. The participants were introduced with legal aspects and practical cases in the field of personal data and privacy in our country, the role of the Authority in the process of handling complaints, as well as regarding most recent developments in this area in the EU.

The Commissioner's Office has published 3 issues of "**I**nformation **a**nd **P**rivacy" magazine (June 2016 – June 2017). This is a periodic publication of the authority, every 6 months, which reflects the main activities of the institution. The magazine aims to raise citizens' awareness to exercise in practice their constitutional rights.

In the context of the Continuous Training Program, 2 seminars were conducted at the School of Magistrates (June 2016 and February 2017) on "Personal data protection in the judiciary system". These seminars were attended by judges from all courts. The Commissioner's Office addressed legal aspects, issues and practical cases resulting from the complaints examined and the administrative investigations conducted, with special focus on the annonymization of personal data in the judiciary system, and the new European legal framework on data protection.
The personnel of the Commissioner's Office received a Tailor-made Training (TMT) in November 2016, funded by "The Netherlands Fellowship Programmes" of EP-Nuffic, part of the Ministry of Foreign Affairs of the Kingdom of Netherlands and implemented by Vrije University of Amsterdam. The training was conducted by academics and researchers, representatives of Dutch Data Protection Authority, lawyers and non-governmental organizations' activists. A general overview on Data Protection Regulation of the EU, which enters into force on May 2018, and legal improvements regarding Directive 95/46/EC were the main topics of the training. Additionally, a few case studies were introduced such as data transfers process and decisions of the European Commission on the level of adequacy in personal data protection, privacy in the age of Big Data and Internet of Things; biometric data; direct marketing; unsolicited phone calls register (Do not call me register); cooperation of law enforcement agencies; handling of citizens' complaints, etc.

The Office of the Commissioner in cooperation with the Rectorate of Tirana University conducted on 23-27 January 2017 the Winter School "Information and Privacy", organized in the context of data protection week. This first edition gathered 60 students, academic and administrative staff of Tirana University. The personnel of the Commissioner's Office introduced attendees with the national legal framework, supervision powers of the Authority, as well as with the new EU General Data Protection Regulation, etc.

The IDP commissioner's Office has introduced its new privacy app "IDP Ankesa", which enables individuals to file a direct complaint from their smart phones with the Office of the Commissioner. Such application involved students of the "Harry Fultz" Institute of Tirana who participated in the competition launched by the IDP Commissioner, and concluded the design of an application user-friendly and very efficient to direct exchanges. It is now available on Play Store.

The Commissioner's Office in cooperation with the State Minister for Innovation and Public Administration organized an activity in the framework of "Internet Safe Day". In this event, was introduced the survey prepared by the Commissioner's Office: "Privacy and security of personal data during the use of social networks by 15-18 year old age group", as well as the "Resolution for the adoption of an international competency framework on Privacy Education", adopted by the 38th International Conference of Data Protection and Privacy Commissioners. The aforementioned survey is the result of 2016s campaign: "Privacy and security of personal data during the use of social networks by teenagers", involving students and teachers from 36 secondary schools.
Additionally, a meeting was held with representatives of Regional Departments and Education Offices of the Country, at the launch of "Privacy and security" awareness campaign, aiming to introduce the "Resolution for the adoption of an international competency framework on Privacy Education", and the "Privacy and security of personal data during the usage of social networks by 15-18 year old group ages" survey prepared by the Commissioner's Office.

International Cooperation

Certification of Albania as a country ensuring an adequate level of personal data protection
The Commissioner Office triggered with representatives of the Data Protection Unit of DG JUST the procedures for certification of Albania as a country ensuring adequate level of personal data protection. To this effect, on 21 June 2016, a bilateral meeting was organised between the representatives of the Commissioner Office and the representatives of Data Protection Unit of DG JUST in Brussels, where it was discussed on the application modalities. The latter was performed jointly with the Ministry of Foreign Affairs, and contained a comprehensive and detailed report of the legal framework and the current situation of data protection in the Republic of Albania, prepared by the Office of the Commissioner.

IDP to host Spring Conference in 2018
Following its application submitted earlier in 2017, IDP Commissioner's Office was appointed as the 2018 host of the European Conference of Data Protection Authorities, and in this regard it prepared and introduced the anticipated details of organization during this year's edition in Cyprus.

Case Handling Workshop 27th edition Handbook
The Commissioner Office introduced during the Spring Conference of Data Protection Authorities held in Budapest, the Handbook prepared by the Office of the Commissioner following the organization of the 27th edition of Case Handling Workshop in 2015 in Tirana. This Handbook could be found in the official website of European Commission (CIRCabc).

Involvement in GPEN
26 Authorities of Data Protection, including the Commissioner Office, joined this year the GPEN Privacy Sweep initiative, (GPEN - Global Privacy Enforcement Network). The purpose of this initiative was the verification of the practices of private and public controllers in the field of information and communication technology. Under the focus this year were the technologies IoT (Internet of Things), wearable devices (fitness trackers), VOD (video on demand), smart TV, smart meters and the respective applications in smart phones.
The Commissioner Office contributed to this initiative through the organisation of verifications of the websites and various applications, such as "Digital Police Station", etc., and the outcomes of these verifications were reported to GPEN coordinators.

The Commissioner Office acceded to the Ad Hoc Committee CAHDATA of the Council of Europe and attended its first plenary meeting of the new mandate, as well as the International Conference of CoE for the promotion of the modernised Convention 108 held in Strasbourg.

Cooperation with Counterpart DPAs
The Commissioner Office has cooperated with counterpart DPAs in exchanging information, implementing agreements and projects. It is worthwhile mentioning the ongoing cooperation with the Italian Data Protection Authority (*Garante*) in the framework of a cooperation agreement with focus on the exchange of information, joint activities and joint inspections.

Support from TAIEX
In the context of the findings of 2015 Country Report with focus on the infringements of privacy and data protection rights of the citizens by the Media, the Office of the Commissioner organized in September 2016, in cooperation with Taiex a "Workshop on Media and Compliance with the Data Protection Principles". The workshop received contributions from prominent international experts in the field of personal data protection and Media.
As of 2017, 5 events, namely 3 expert missions and 2 study visits with focus on the new European legal framework of data protection and the possible amendments to our national legislation, have already been approved and are currently being organized.

ANDORRA / ANDORRE

ANDORRAN COUNTRY REPORT ON THE RECENT DEVELOPMENTS AT NATIONAL LEVEL IN THE DATA PROTECTION FIELD.

Since 2010, where the last changes were made, Andorra hasn't modified its Law and regulation on Legal Protection of Personal Data.

However, the follow legal instruments have been passed which contain specific provisions on personal data, where the Andorran Authority in Data Protection (henceforth 'this Authority') has ruled out Assessment Reports.

- Regulation on the Gambling regulator council.
- Regulation on Sportsmen personal data file and international transfer by the Anti-doping Andorran Agency.
- Automated fiscal information exchange Act

Furthermore, this authority has also given legal Opinions on the following draft bills:

- Quadrennial Statistics Plan, under the request of the Finance Ministry.
- Rights and Obligations of medical patients and Clinical History Act, under the request of the Health Ministry.

Additionnally, this authority has also stated its opinion on other subjects such as the "Report on the Use of participation data in election campaings" under the request of the Andorran Parliament.

In turn, on January 28th, on the occasion of the European Day of Protection of Personal Data, this Authority published a Hanbook of Data Protection in Work Environtment.

Finally, this Authority has also promoted and organized a series of seminars and workshops addressed to all kind of audiences:

- Bar Association
- Superior Council of Justice
- Ministry of Social Affairs
- University of Andorra
- Youth Centres

ARMENIA / ARMENIE

Major Developments in the Personal Data Protection Field in Armenia as of May, 2017

The major developments in the Republic of Armenia with regard to personal data protection since June, 2016 are the following:

The Agency adopted the list of countries with adequate level of protection of personal data

- On February 17, 2017, the RA Personal data Protection Agency adopted decision, by which the list of countries with adequate level of protection of personal data was established. The list includes 50 countries, which were recognized as providing sufficient level of protection of personal data based on the following criteria: the country should simultaneously 1) have ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108 Convention), 2) have a Law on the protection of personal data or other document, which is comparable with the status of law (relevant legislation) and 3) have an authorized state body for the protection of personal data.

Amendments in the RA Law on Personal Data Protection

1. In December 2016, amendments were made in the RA Laws on Personal data Protection, the provision of the Law, which provided that the restrictions of the Law did not apply to the personal data processed for journalistic purposes or for the purposes of artistic or literary expression, was repealed.

2. Under the Freedom of Information legislation reforms changes in the RA Law on PDP were drafted to ensure everyone's right to receive information about himself/herself (information about property, rights, freedoms, duties, limitations of rights or information on liability). The Draft is in the stage of public discussions.

3. On February 16, 2017, the Procedure of electronic transfer of personal data from databases of state and self-governmental bodies was established by the RA Government's decision.

- **Completed tasks by the Agency**

Consultations, conferences, notifications
As of May 1, 2017 since June 2017, the Agency
- Provided consulatations to over 120 legal and natural persons;
- Conducted 34 workshops, public meetings and interviews:
- Received over 100 notifications of processing of personal data.

Administrative proceedings
As of May 1, 2017 since June 2017, the Agency initaited 16 administrative cases upon an application or by the Agency's initiative.

Two administrative cases covered 20 schools of Yerevan. They checked lawfulness of video surveillance in 20 schools (in classrooms and working cabinets) was verified. During the proceedings of the Agency found that there are different violations of the data protection legislation in different schools - in some cases the principle of lawfulness of data processing was violated, in some cases and mostly the principle of proportionality of data processing was violated and in some cases the school administrations had not provided for proper security measures for processing personal data. As a result, with the consultation and assistance of the Agency administrations of 20 schools eliminated the identified violations and operated video surveillance strictly according to the DP law requirements.

Guidelines (soft laws)

In the given period the Agency developed and published 4 guidelines:

- A guideline on the protection of children's personal data,
- A guideline on the protection of personal data in labor relations,
- Two guidelines on protection of personal data in social networks

AUSTRIA / AUTRICHE

Major developments in the data protection field in Austria 2016/2017

- The annual report of the Austrian Data Protection Authority (Annual Report 2016) will soon be available in German at https://www.dsb.gv.at/dokumente.
- In its decision of 25 February 2016, E2424/2015, the Austrian Constitutional Court ruled that the publication of personal data in the context of agricultural subsidies on the internet does not violate Art. 7 and 8 of the Charta of Fundamental Rights of the EU.
- Legislation/legislative procedure:
    - the Police State Security Act (*Polizeiliches Staatsschutzgesetz*) which gives the intelligence branch of the police broader competences; entered into force on 1 July 2016; the competences of the DPA remain untouched
    - the Austrian Parliament is considering an amendment to the Police Cooperation Act (*Polizeikooperationsgesetz*) allowing the enhanced exchange of personal data with police authorities in other states. The draft is available in German at https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01612/fname_630015.pdf.

AZERBAIJAN / AZERBAÏDJAN

This is information on the major developments in the data protection field in Azerbaijan since our country became the Party to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. There are too many normative legal acts, Laws of the Republic of Azerbaijan, Statements of the President of the Republic of Azerbaijan, Decrees of the Cabinet of Ministers of the Republic of Azerbaijan in the data protection field and the main of them is the Law on data protection.

The main of some normative legal acts is the Law of the Republic of Azerbaijan "On personal data" which regulates relationships associated with collection, processing and protection of personal data, formation of personal data section of national information space as well as matters related to transfrontier transfer of personal data and sets out rights and obligations of the state and local self-government authorities, legal and natural persons operating in this field.

Main purpose of the mentioned Law is composing of determination of legislative grounds and general principles of collection, processing and protection of personal data, rules and requirements of the state regulation in that sphere, rules of formation of personal data in information resources, establishing of information systems, issuance and transfer of information, fundamental human and citizens' rights, freedoms and grounds for their liability, including protection of the right to a private and family life.

Legislation of the Republic of Azerbaijan in the sphere of personal data

1. Legislation of the Republic of Azerbaijan in the sphere of personal data shall be composed of the Constitution of the Republic of Azerbaijan, international agreement which the Republic of Azerbaijan is a party to, present Law and other normative legal acts.

2. For the purposes of provision of national security of the Republic of Azerbaijan as well as lawfulness, rules for collection of personal data in connection with enforcement of intelligence and counterintelligence, operative-research activities, protection of personal data regarded to state secret and collected in national archival fund shall be defined by the legislation of the Republic of Azerbaijan.

3. Provisions of the present Law shall not apply to collection and processing of personal data by natural persons for personal and family needs.

Main principles of collection, processing and protection of personal data

1. Formation of information resources, establishment of their information systems shall be carried out in accordance with principles of lawfulness, confidentiality, combination of voluntariness with compulsion complying with fundamental human and citizens' rights and freedoms enshrined in the Constitution of the Republic of Azerbaijan.

2. Posing the treat to life and health of person, degrading his/her honour and dignity shall not be allowed in the course of collection, processing and protection of personal data.

Legal regime and protection of personal data

1. Personal data shall be subject to protection from the moment of their collection and, for those purposes, they shall be divided into confidential and public categories depending on type of access (acquisition).

2. Confidential personal data shall be subject to protection on the level corresponding to the requirements provided for in the legislation by owners, operators and users who have acquired a right of access to those data. Except for cases provided for in the legislation, confidential personal data may be transferred to third persons only on the basis of consent of the subject entity.

3. Category of public personal data shall include data on subject entity, which were depersonalized, as provided, disclosed by itself or entered, upon its consent, into information systems established for public use. Surname, given name and patronymic of person shall be regarded to permanently available public personal data. Provision of confidentiality of personal data of public category shall not be required.

4. Data of specific category may be regarded both to the category of confidential and category of public personal data with due regard to their features and requirements of Article 11.1 (Article 11.1. The owner or operator shall be entitled to receive from subject entity only those personal data which are required for achievement of processing purposes.) of the present Law.

5. Protection of personal data shall be ensured by owners and operators. Natural persons acting in the sphere of collection, processing and protection of personal data shall be obliged to undertake written statement for non-disclosure of those data within the period of their activity and upon their retirement.

6. For the purposes of enforcement of informational provision of the society in the sphere of telecommunications, mail service, address and other spheres, data provided by the subject entity about itself (surname, given name, patronymic, date and place of birth, sex, citizenship, phone number and e-mail address, place of residence and seat, qualification and place of employment, type of activity, marital status, photo and other data) may be entered into information systems with the written consent of that subject entity.

7. In the course of entry of personal data into information systems of public use from bare sources, operator shall be obliged to inform the subject entity about composition of those data entered and source of their acquisition. Those data shall be immediately excluded from that information system on the basis of written request of the subject entity, court or relevant authority of executive power.

8. Owner or operator shall be obliged to carry out organizational and technical measures guaranteeing provision of personal data protection (including their accidental and unauthorized deletion, loss, unauthorized access, alteration and other cases).

9. Requirements for protection of personal data shall be defined by the relevant authority of executive power.

10. Rules of archiving of personal data shall be defined by the relevant legislation of the Republic of Azerbaijan.

Main forms of state regulation in the sphere of collection, processing and protection of personal data

Measures of state regulation in the sphere of collection, processing and protection of personal data shall be as follows:

1. formation of section of personal data in national information space and provision of its protection, assessment of threats and protection level of that sphere;

2. determination of legal base of collection and processing of personal data;

3. provision of fundamental human and citizens' rights and freedoms in the course of collection and processing of personal data;

4. licensing of the activity for collection and processing of personal data;

5. performance of the state registration of information systems of personal data;

6. certification of information systems of personal data as well as respective means of information technologies;

7. standartization of legal and technical documenting in the sphere of establishment and application of information systems of personal data;

8. exercise of state expert examination of information resources and personal data systems and their project documents;

9. state regulation in the sphere of establishment of state interdepartamental information systems of personal data and of their management.

Rights of the subject entity

1. Subject entity shall be entitled to:

1.1. acquire information on availability of personal data about him/her from the owner or operator of the information system;

1.2. require legal substantiation of collection, processing and transfer to third persons of personal data about him/her available in the information system and acquire information about legal consequences which may emerge as a result of collection, processing and transfer to third persons of such personal data;

1.3. get acquainted with the content of personal data about him/her accumulated in the information system;

1.4. be aware of purpose of collection and processing of personal data about him/her in the information system, terms, processing methods, range of persons authorized to get acquainted with his/her personal data, including information systems providing for performance of information exchange;

1.5. require alteration or deletion of any personal data about him/her collected in the information system of personal data as well as lodge applications on transfer of such data, as provided, to the archive, except for cases provided for in the legislation;

1.6. require a prohibition of collection and processing of personal data about him/her;

1.7. acquire information on sources of acquisition of any personal data about him/her collected in the information systems, require proof of lawfulness of such data;

1.8. require protection of any personal data about him/her collected in the information systems;

1.9. acquire information on availability of certificates of compliance and of passage of state expert examination of information systems where any personal data about him/her are collected;

1.10. use other rights set forth in the present Law and other normative legal acts of the Republic of Azerbaijan.

2. Subject entity shall be entitled to object against collection and processing of personal data about him/her, except for cases where collection and processing of data are of mandatory nature,

as provided for in the legislation. Objection of subject entity shall be communicated in writing to the owner or operator. Substantiation of objection of the subject entity shall not be required. Upon receipt of such objection, owner or operator shall be obliged to suspend the collection and processing of personal data immediately.

3. In the event that decision taken as a result of collection and processing of personal data through information technologies breaches interests of the subject entity, he/she shall be entitled to object against collection and processing of such data by means of mentioned method, except for cases which are of mandatory nature, as provided for in the legislation. In the event that owner or operator receives an objection against processing of personal data through information technologies, they shall be obliged to receive consent of the subject entity for processing of data through the other method or to suspend processing of personal data immediately.

4. In the event that rights of the subject entity are breached as a result of illegal collection and processing of personal data about him/her as well as failure to ensure their protection as well as failure to comply with the requirements of the present Law, he/she shall be entitled to lodge complaint to the relevant authority of executive power or to the court as well as require, through the court proceedings, reimbursement of moral and material damage caused to him/her.

5. Subject entity shall carry out rights set forth in the present Law through the communication to the owner or operator of written statement drawn up on paper and certifying identity of the document or through the communication of electronic request with reinforced electronic signature.

Consent of the subject entity for collection and processing of personal data about him/her

1. Except for cases of mandatory collection and processing of personal data, as provided for in the legislation of the Republic of Azerbaijan, collection and processing of personal data about any person shall be allowed only with the written consent of the subject entity, including consent in the form of electronic document with reinforced electronic signature or on the basis of written data submitted by him/her.

2. Written consent of the subject entity for processing of personal data shall include the following:

2.1. data allowing to identify the identity of the subject entity;

2.2. data allowing to identify the owner or operator acquiring the consent of the subject entity;

2.3. purpose of collection and processing of personal data;

2.4. list of personal data, consent of the subject entity to which is granted and of operations for their processing;

2.5. validity period of consent of the subject entity and terms and conditions of its withdrawal;

2.6. terms and conditions of deletion or archiving of collected personal data about the subject entity, as provided for in the legislation, upon completion of fixed period of storage of personal data in the respective information system or upon his/her death.

3. In case of death of subject entity, or declaration of him/her as dead, as provided for in the legislation of the Republic of Azerbaijan, recognition of him/her as missing, incapable as well as underaged, absence of his/her right to freely express the consent required by the present Law, consent shall be granted by his/her heirs, authorized representatives, parents or guardians.

4. Owner or operator shall be obliged to submit proof of acquisition of consent of the subject entity for collection and processing of his/her personal data. Processing of personal data about dead persons may be carried out in cases provided for in the legislation, if no prohibition was put on processing of such data *inter vivos* of the subject entity.

5. Owner or operator performing collection and processing of public personal data shall be obliged to submit proof that such data are regarded to the category of public personal data.

Registration of information systems of personal data

1. Information systems of personal data, including information systems which were existing prior to entry of the present Law into force, shall be subject to state registration in the relevant authority of executive power. Rules of state registration and liquidation of state registration of information systems of personal data shall be approved by the relevant authority of executive power.

2. Except for the purposes of provision of national security of the Republic of Azerbaijan as well as lawfulness, rules for collection of personal data in connection with enforcement of intelligence and counterintelligence, operative-research activities, protection of personal data regarded to state secret and collected in national archival fund shall be defined by the legislation of the Republic of Azerbaijan, collection and processing of personal data without state registration of information system of personal data shall be prohibited.

3. Following information systems of personal data shall not require state registration:

3.1. information system of personal data regarded to state secret in accordance with the legislation of the Republic of Azerbaijan on state secret;

3.2. information system of personal data regarded to subject entities who are in labor relationships with the owner or operator or required for their access to the working territory;

3.3. information systems of personal data defined by the relevant authority of executive power and established depending on purpose of processing of personal data and maximal limit of number of subject entities in cases, which do not require state registration.

Division of national information space by personal data

1. Formation, use and development of division of national information space by personal data shall be carried out on the basis of integrated scientific and technical concept.

2. For provision of sustainable and protected interaction of information systems of personal data in national information space and prevention of abhesion in their means of provision in this sphere, information technology and safety standards shall apply.

3. With the purpose of agreement of data about the same subject entity located in different information systems distributed in the section of personal data of national information space, provision of prevention of fragmentation and iteration in this field, personal identification number shall apply. Except for cases provided for in the legislation, amalgamation of information systems and resources of personal data belonging to different owners and having different assignment shall not be allowed.

4. Rules of inclusion and use of personal identification number in the information systems of personal data shall be defined by the relevant authority of executive power.

Also on the basis of Decree of the President of the Republic of Azerbaijan “On Appliance of the Law on Personal Data” dated 4 June, 2010, number 275 there was prepared “The Requirements concerning the protection of personal data” and they were approved by the Cabinet of Ministries of the Republic of Azerbaijan dated 6 September, 2010, number 161. These Rules are regulates relations generated during collecting, using, spreading and giving by operator or proprietor of such personal data or certain information systems.

According to the Decree of the President of the Republic of Azerbaijan on appliance of the Law of the Republic of Azerbaijan "On personal data" dated 13 of December, 2010, number 361 the relevant authority of executive power shall examine compliance of collection, processing and protection of personal data in the information systems included into the state register with the requirements of the present Law as well as compliance of those data and methods of their processing with declared purposes of information system. The functions of the relevant authority mentioned above are carried out within the powers by the State Security Service of the Republic of Azerbaijan, the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, the Ministry of Internal Affairs of the Republic of Azerbaijan, the Ministry of Justice of the Republic of Azerbaijan and Special Service of the State Protection of the Republic of Azerbaijan.

In accordance with the Decree of the President of the Republic of Azerbaijan On appliance of the “State Program On Improving communications and information systems in the Republic of Azerbaijan during 2005-2008 (Electronic Azerbaijan)” dated 21 of October, 2005, number 1055 there was established the State Register of State Information resources and Information Systems of Personal Data of the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan.

In addition by the Decree dated 28 January, 2006, number 27 of the Cabinet of Ministers of the Republic of Azerbaijan “On the approval of some of the normative legal acts for electronic signature and electronic document in the Republic of Azerbaijan” there have been defined “The Rules for electronic signature validation”, “The Rules on State authorities and local government bodies to use the electronic signature”, “The Rules on registration and accreditation of the Center (certificate services center) providing the certificates for electronic signatures and services on the use of signatures”, “The Rules on Providing the certificate services, giving the certificates and carry out registry of certificate”, “The Rules on Exchange of electronic documents”.

Also by the Decree of the Cabinet of Ministers of the Republic of Azerbaijan on adoption "The Rules of using and introduction of personal identification number of personal data to information systems" dated 4 April, 2011, number 49, which was prepared according to The Law of the Republic of Azerbaijan “On personal data”, there was defined such issues as a single unique combination of letters and numbers which allows to clearly define in the prescribed manner corresponding and submitted data about persons whom about the personal identification number was included in to the Information systems of personal data.

BOSNA I HERCEGOVINA
Agencija za zaštitu ličnih/osobnih
podataka u Bosni i Hercegovini
S a r a j e v o

БОСНА И ХЕРЦЕГОВИНА
Агенција за заштиту личних података
у Босни и Херцеговини
С а р а ј е в о

BOSNIA AND HERZEGOVINA / BOSNIE ET HERZEGOVINE

No. 04-37-11-33-25/17
Date, May 26, 2017

34. Plenary meeting T-PD
T-PD Secretariat
dataprotection@coe.int

Subject: **The most important activities in the field of personal data protection in Bosnia and Herzegovina for the period July 2016 – May 2017**

The Agency for Personal Data Protection in Bosnia and Herzegovina was established by the Law on Personal Data Protection (Official Gazette, no. 49/06) and commenced operations in June 2008. The Law on Amendments to the Law on Personal Data Protection ("Official Gazette" No.76 / 11) adopted by the Parliamentary Assembly of Bosnia and Herzegovina in 2011. The Ordinance on internal organization and job classification systematized 45 working places in the Agency. The Agency currently employs 26 employees.

Normative part

One of the legal obligations of the Agency is to monitor the situation in the field of protection of personal data and, in this respect, to make proposals, initiatives and opinions. During the reporting period, the Agency has prepared the opinion to the Ministry of Justice to the Draft Law on Amendments to the Law on Salaries and Other Compensations in Judicial and Prosecutorial Institutions at the BiH level, opinion to the Ministry of Justice to the draft Law on the Appointment Procedure on the level of BiH institutions, opinion to the Ministry of Communications and Transport on Draft Law on Amendments to the Law on International and Inter-entity Road Transport, opinion to the Ministry of Security on proposal of the Ordinance on the central database on foreigners, opinion to the Ministry of Education, Science and Youth of Sarajevo Canton on the Draft Law on Higher Education, and the amendment to the opinion regarding the same draft law, then the opinion to the Ministry of Civil Affairs on the proposed Law on Amendments to the Law on Medicines and Medical Devices, opinion to the Deposit Insurance Agency of Bosnia and Herzegovina on proposed Law on Amendments to the Law on Deposit Insurance in Banks of Bosnia and Herzegovina, opinion to the Indirect Taxation Authority on the draft Law on Amendments to the Law on the Indirect Taxation Administration, as well as the opinion on the proposed Law on Amendments to the Law on Value Added Tax, two opinions to the Deposit Insurance Agency of Bosnia and Herzegovina on the proposal of the Law on Deposit Insurance in Banks of Bosnia and Herzegovina, opinion to the Ministry of Physical Planning, Construction and Environmental Protection of Sarajevo Canton on the proposed Law on Management of the Common Parts of Building. In total, the Agency issued 12 opinions on various draft laws and other administrative acts.

Giving expert opinions on the requirements of the controller and personal data subjects is in constant increase. A large number of requests for an opinion on the requirements of the public and private sector testifies about increasing the awareness of all entities on personal data protection. On the requests of the public and private sector 140 opinions were issued and 12 opinions and one reply issued on the transfer of personal data abroad. On the requirements of natural and legal persons two expert opinions and two response were composed.

Through the inspection, the Agency shall supervise the fulfilment of obligations stipulated by the Law on Personal Data Protection. In carrying out its regular surveillance activities, in the reporting period the Agency carried out 54 regular and 26 extraordinary inspections and issued 15 decisions and one conclusion after the completed regular inspections.

In the reporting period 10 judgments of the Court of BiH were issued in favour of the Agency, delivered 5 response to the complaint, made three requests for review of the court decision and composed one information at the request of the Court.
According to the Agency's activities conducted in the reporting period, the state of personal data protection in our country could be described as satisfactory. This is evidenced by a significant increase of number of submitted complaints of citizens indicating increased awareness of the importance of personal data protection. In the reporting period 67 decision on the complaint were composed, mostly against public entities, as well as other controllers, such as banks, micro-credit organizations and other economic entities and individuals and performed 116 activities per case in the complaint procedure.

The Agency has started issuing misdemeanour warrants in 2011 and in the reporting period issued 17 misdemeanour warrants.

The Agency also continued with the activities of the training sessions on the importance of personal data protection in the public sector on the whole territory of BiH. During the reporting period, 11 trainings and lectures were held.

Cooperation with media

The Agency regularly informs media about its competences and activities, promoting the work of the Agency and inform the public regarding the processing and protection of personal data. The Agency normally responded to all media inquiries and reported on time by all available means of public information and published opinions and decisions on the official website of the Agency, as well as through the Help Desk.

In this respect, there was a press conference on the occasion of the European Data Protection Day, January 28, 2017. At various inquiries of print and electronic media 10 written responses were given, 6 statement and it was 5 media appearances. Through Help Desk of the Agency 479 inquiries of citizens were replied. Inquiries referred to the possibility of transfer of data abroad, obtaining insights into documents, video surveillance, processing identification number, the establishment of a database of personal data, registration of records, data security plan, the filing of the complaint, the legal basis for giving personal data to a third party, registration of records upon the letter of the Agency, collection complement, filing complaints, application procedures and documentation that may be required, i.e. performing insight, request for a copy of identity card, delivery of data to the foreign employer, publication of incomes in media.

Web site of the Agency is regularly updated with the necessary content which shows commitment to the transparent operation of the Agency. In the reporting period there were 13892 visits to the Web site of the Agency. In media and on the Internet 35 articles related to the Agency's activities and personal data protection were published.

European integrations

Within the activities of providing a response to the European Commission and accompanying legal documents to be submitted with the answers to the Questionnaire, entry of 19 responses to questions relating to the Agency for Personal Data Protection in of BiH in the information system of the Directorate for European Integration of the Council of Ministers (CoM DEI) was carried out and revision of English translation of the Law on Personal Data Protection performed in accordance with the Manual of DEI BiH of the Council of Ministries for translation of legal regulations in of BiH.

Director
Petar Kovačević

BULGARIA / BULGARIE

MAIN DEVELOPMENTS IN THE SPHERE OF PERSONAL DATA PROTECTION IN

The Commission for Personal Data Protection (CPDP) is the national supervisory body responsible for protection of personal data in the Republic of Bulgaria. Being the only data protection authority (DPA) in the country, the CPDP has a wide range of powers and performs a number of different tasks, such as investigations, corrective measures, awareness-raising and information campaigns, international cooperation, training, etc.
Overall in 2016 the CPDP handled 650 complaints, carried out 844 inspections, imposed administrative penalties totaling BGN 265 000 and issued 9 compulsory instructions to data controllers.

The main developments concerning data protection in Bulgaria fall within the following main area of DPA's duties:

Sectoral inspections
Back in 2015 CPDP identified the need to change the approach for selecting personal data controllers to be inspected and reverted to sectoral inspections. 2016 witnessed the first of its kind sectoral inspection in the sphere of education. The inspection covered a number of educational institutions (kindergartens, primary and secondary level schools – state and private, universities) as well as the Ministry of Education and Science. The Commission recommended a series of measures that need to be undertaken in the sphere of education to provide compliance with the current legal framework of data protection in Bulgaria.

Proceedings with political parties
Bulgarian Electoral Law requires political parties to collect certain number of supporting signatures (including name, address of living and personal identity number) of citizens to confirm that the political subject are recognized by the citizens and this is prerequisite for their registration in national elections. In 2016 the Commission for Personal Data Protection received 220 complaints against political entities in connection with the presidential elections. The Commission undertook all necessary measures to ascertain the validity of the complaints. In order to prevent future similar mishandlings of personal data the CPDP proposed legal and organizational measures, which include:

- Submission of document proving that the political entity is a registered data controller when registering with the National Electoral Commission before the elections;
- Introduction of "date of signature" column in the signature lists with citizens supporting the respective political entity;
- Introduction in the electoral Code of Conduct of the possibility identification of the data subject to be required prior to signing the lists for support of the respective political entity.

Adoption of Strategy for Development in the Area of Personal Data Protection (Horizon 2022)
In order to facilitate the preparation for the GDPR implementation in Bulgaria and the everyday work of the institution, the CPDP developed and adopted a development strategy. It defines the mission and vision of the CPDP and sets the main strategic goals of the institution. The strategy also introduces targeted policies for their achievement. Among the main policies underlying the strategy are the policy of accountability and control, the partnership policy, the policy of European cohesion and the prevention policy. The action plan includes concrete activities for implementing all policies and activity owners for adequate distribution of tasks.

Preparation of the CPDP for jointly hosting the 2018 International Conference of Data Protection and Privacy Commissioners
In 2016 the CPDP and the EDPS submitted a joint application to host the 2018 ICDPPC. The application was approved by the Executive Committee at the beginning of 2017. The CPDP is in the process of preparation for the event which will take place in October 2018 simultaneously in Brussels and Sofia. More details will be presented at the next 2017 ICDPPC conference in Hong Kong.

Training of data controllers

In 2016 the CPDP again put an emphasis on prevention. One of the main tools for implementing the policy of prevention is training for personal data controllers and processors. This is a statutory activity of the CPDP laid down in Article 10 of the Personal Data Protection Act, which is systematically built on every year.

A total of 12 training seminars with 420 participants were held in 2016. Of these, 4 were for representatives of institutions which have access to the National Schengen Information System, 3 were for representatives of judiciary, 3 training events for accredited adoption service providers, 1training for the academic community and 1training for young diplomats.

Awareness raising and cooperation

In 2016 the CPDP continued its awareness raising policy with focus of the incoming GDPR implementation. The Commission published on its website dedicated information materials on GDPR topics such as the obligations of data controllers, the role and responsibility of the data protection officer, the rights of the data subjects and consent as a legal ground for personal data processing.

CYPRUS / CHIPRE

Major developments in the data protection field

EU's General Data Protection Regulation (GDPR) and Data Protection Directive for the police and criminal justice sector

The Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, entered into force on 25 May 2016. Its implementation will start 25 May 2018 and the Regulation will be directly applicable in all member states of the European Union.

Cyprus, as a MS of the EU started in 2016 the preparation for the application of the Regulation. Both public and private organisations will have to make use of the two-year period provided by the Regulation to be ready to implement it on 24 May 2018. To this end, the Office of the Commissioner issued guidance to data controllers outlining ten actions that need to be taken by them in the course of their preparation and has further carried out training sessions to both the public and the private sector in order to prepare them at all levels to implement the new European framework.

Moreover, the Office of the Commissioner is currently preparing the draft law on the implementation of certain provisions of the Regulation.

The European Directive 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, designates the Data Protection Commissioner as the competent national supervisory authority. Following a consultation with the Ministry of Justice, the Office of the Commissioner works with the Police to prepare a draft law for the transposition of the Directive.

Law regulating the right of access to public sector information

Following a public consultation in 2013, the Ministry of Justice presented a draft law regulating the right of citizens to access public sector documents and information. The law aims at promoting transparency and accountability principles, as well as the most effective oversight of acts and decisions taken by public and semi-public authorities. The implementation of this law will be entrusted to the Data Protection Commissioner, who will subsequently become Information Commissioner, once the law will be enacted.

The examination of the draft law started in 2016 by the Parliamentary Commission of legal affairs and is rapidly advancing. Discussions demonstrated the sound support of the draft law by all parties involved and it is expected to be adopted, at the latest, by September 2017.

The DPA has asked for significant budget and staff increases due to the implementation of the freedom of information law and the GDPR. Decision has been taken by the Ministry of Finance to increase the staff by four officers in order to comply with its future functions and principal activities as well as to be prepared for the GDPR.

Cyprus Chairmanship of the Committee of Ministers of the Council of Europe

Cyprus assumed the Chairmanship of the Committee of Ministers for the fifth time, from 22 November 2016 until 19 May 2017. Under the aegis of the Cyprus chairmanship, the Office of the Commissioner organised various activities: a public debate with the Commissioner for Human Rights, the Commissioner of Children's Rights and the Financial Ombudsman to present their competences and raise awareness among the citizens, a series of events related to the Data Protection Day and the Spring Conference of European Data Protection Authorities.

Spring Conference of European Data Protection Authorities 2017

The Office of the Commissioner hosted on 27-28 April in Limassol the 2017 edition of the Spring Conference of European DPAs. Limassol Conference was attended by more than 80 participants, gathered to discuss, among others, raising awareness, transparency in the Cloud, Law Enforcement

Authorities' access to data and genomic research. The conference adopted two Resolutions, one of which relates to the modernisation Convention 108. In their resolution, the European DPAs encouraged the negotiating parties to renew their efforts to find appropriate final solutions to the outstanding issues and call upon the governments of Council of Europe Member States and the European Union to reach a political agreement at the 127th Ministerial Session of the Committee of Ministers to be held in Nicosia on 19 May 2017, enabling a rapid finalisation of the modernisation. More information about the Conference is available here.

Memorandum of Understanding and Cooperation

In May 2017 the Commissioner for Personal Data Protection and the Commissioner of Electronic Communications and Postal Regulation signed a Memorandum of Understanding and Cooperation for the purpose of regulating the application of article 98a of the Electronic Communications and Postal Regulation law and the Decree on the notification of data breaches by electronic communications service providers. The purpose of the Memorandum is to establish a framework for the process of adopting and implementing appropriate mechanisms for more efficient and effective cooperation between the two Commissioners in the reception and processing of data breaches cases by providers of publicly available electronic communications services.

Guidelines and opinions issued by the Commissioner

Guidelines on the use of video-surveillance in public places

The preparation of new revised guidelines appeared to be necessary to respond to the need of municipal authorities to fight against increasing criminal incidents and vandalism in their communities. The guidelines recalled the need to regulate the use of video-surveillance in public places by a specific law and the obligations of data controllers to take the necessary measures for the security of the data. Where the intended processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate the origin, nature, particularity and severity of that risk.

Guidelines to insurance companies

The guidelines set out the legal requirements to be afforded by insurance companies when processing personal data of their clients, including health data. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. Where possible, the data should be collected only from the data subject and information should be provided when data is collected from other sources. The guidelines further tackled the new obligation of the insurance companies deriving from the GDPR on the right of data portability, which is of particular relevance to the insurance sector.

Opinion on the use of Polygraph testing in the context of employment

The DPA issued an opinion on the legitimacy of the use of Polygraph testing in the context of employment. Polygraph testing purport to measure the truthfulness of a person's statements by tracking bodily functions such as blood pressure, heart rate and perspiration. In the employment context the tests could be used by employers to assess the character and personality of an employee or a job applicant. The DPA clearly resolved in its opinion that the use of such tests in the employment context is not allowed, arguing that the processing is disproportionate in relation to assessing employees' or a job applicants' personality and it is an interference with the right to respect for their private life and human dignity. Moreover, the use of Polygraph testing requires the processing of health data which is prohibited, as it is not expressly provided for by national law. The consent of the employees or job applicants does not lift the prohibition of the processing in the specific case.

Opinion on the recording and broadcasting of councils' meetings

An opinion was delivered addressing the issue of publication of the recording of the meetings on the Municipalities and Communities websites, as well as their live broadcasting on the Internet. The DPA considered that such publication and broadcasting is disproportionate in relation to the purpose of the processing and may entail the disclosure of personal data that is not in line with the law. Nonetheless, Municipalities and Communities Councils may, if they wish, audio record the meetings for the preparation of the meeting's report, provided that all stakeholders have given their consent or provided that legitimate interests prevail. The DPA further underlined that audio recordings should be kept safely and be deleted after a short period of time.

Judgment on biometric data: dismissal of an appeal concerning the collection and processing of fingerprints in the context of employment

The Administrative Court, by its decision of 19 May 2017 (No. 1930/2012), upheld the Data Protection Commissioner's decision of 2012, imposing to a Private Hospital the administrative sanction of the interruption of a biometric system, which processed employees' fingerprints and subsequently the destruction of the relevant data. The Court reaffirmed the decision of the Commissioner, which held that the fingerprint system, set up by the applicant to check the time of arrival and departure of the employees, was in violation of the principle of proportionality provided for in article 4(1)(c) of the Data Protection Law. The Court further held that the use of biometric systems to check employees' working hours is a disproportionate measure and an intrusion into employees' privacy.

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

Major developments in the data protection field in the Czech Republic since June 2016

1. The bill, called misleadingly *"the law amending the Police of the Czech Republic Act and the General Inspection of Security Forces Act*", in fact however a draft act on DNA national database should have legalized the present, unsatisfactory and unclear, situation that basically gave preference to the security aspect ether than the privacy view. The Czech DPA could not agree with the enormous extent of the national DNA database (it was designed to include all intentional criminal acts, except of four types of offences, instead of crimes where biological footprint was left, i.e. violent, property, and vice crimes), neither with the enormous retention period (up to 80 years from the committing of the respective crime).

2. The Government Resolution No. 820 of 14 November 2012 was implemented as of January 2013 covering all draft laws and draft legal regulations with countrywide effect (laws, government regulations, and decrees), and assessments of how the proposed law would impact privacy (DPIA). Continuous awareness work in relation to the purpose and form of DPIA in 2016 already brought fruits at some supreme administrative courts and authorities, like for example at the State Office for Nuclear Safety, or specifically in case of the draft amendment of the Building Society Account law proposed by the Ministry of Finance.

3. Following the decision of the Supreme Administrative Court, the purpose of the operation of a video surveillance device for property protection represents only a gathering of data to be – if needed – transferred to the eligible authorities for eventual proceedings and not for the purpose of their disclosure in itself. Investigation and prosecution of crimes, offences included, is completely under the competency of government bodies. The right of property protection should be materialized through the handover of the data collected to the Police of the Czech Republic. Publication of the data gathered in such a way on the social networks, irrespective of leading it subsequently to the detection of the offender or not, constitutes already the surpassing of the set limit.

DANEMARK / DENMARK

Country report Denmark

Adaptation and amendments of legislation entailed by the GDPR

During the past year, the Ministry of Justice in Denmark has analyzed the consequences of the General Data Protection Regulation (GDPR) for existing Danish law and legislation. A number of ministries and authorities have contributed to this work. The result has been published in a comprehensive report. You can find the report in Danish here:

http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2017/nye-regler-styrker-beskyttelsen-af-persondata-i-europa

Later this fall the parliament is expected to adopt necessary legislative changes as a consequence of the GDPR, including the act, which will establish the competent authority to enforce GDPR.

Directive (EU) 2016/680

Besides the GDPR, the new data protection framework also include the directive 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.

In Denmark the law implementing the directive has been agreed upon end of April this year. The reason for this early adoption is that the implementation of the directive in Danish legislation has become a prerequisite for Denmark obtaining a new affiliation agreement with Europol. Because of a treaty proviso Denmark will formally and effectively resign from Europol in May 2017, when the Europol cooperation is moved from EU´s third pillar to the first pillar. So as of 1 May 2017 the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties are obliged to follow the law implementing the directive and the Danish DPA acts as a supervisory authority according to the act/directive.

Current cases

Use of bodycams by security guards:

The DPA received a notification in 2016 about the processing of personal data from G4S who wanted to use bodycams in connection with the exercise of security activities.

The background for the review is an increasing tendency to general turmoil, violent episodes, as well as other verbal and physical episodes towards the G4S security staff.

To meet this trend G4S wants to use body cams in places where the staff are assessed to be particularly exposed.

The DPA gave G4S a three-year license for the processing of personal data in question. The DPA found that the processing in the specific case can be done within the framework of the Act on Processing of Personal Data § 8, 4. The DPA also emphasized that bodycams can only be used in cases where the G4S finds it particular beneficial and effective and estimates that it has a preventive effect and are important for maintaining peace, order and security

It follows from the personal data sheet's requirement for good data processing practices that the employees - including new employees - must be informed of all the purposes of using bodycams. This information must be given in advance. Recordings must be deleted after 14 days.

School going through private computers and tablets

In 2016, the DPA dealt with a case where two parents complained to the agency that the management at a school had gone through the search history on their son's private PCs and / or tablets.

In November 2015, the school leader and vice inspector interrupted teaching in a 7th grade and asked 9 boys to go to an adjacent room and bring their private PCs and / or tablets.

According to the school, the background was that the management of the school previously had been contacted by a 7th grade parent who had spoken to several other parents who had confirmed that they had heard that porn was watched during school hours.

School management therefore reviewed the search history of the 9-boy's PCs and / or tablets with a view to finding out if the boys had visited websites with pornographic content. During the review, nothing was found.

The Danish Data Protection Agency stated inter alia the following:

• The DPA considers the reading or review of 9 students' search history as processing of personal data covered by the Act on processing of personal data.
• The Agency assumes that the review of the students search history is a processing of common non-sensitive personal data, which shall be in accordance with section 6 of the Act on processing of personal data.
• The processing must also meet the basic requirements principles of fairness and proportionality in section 5 of the Act on processing of personal data.
• In the opinion of the DPA, when assessing the legality of the treatment that has been done the DPA have considered that it were private-owned equipment, and thus not equipment that the school had ownership or availability of.
• It should also be considered that the search history of the investigated devices could also include searches made outside school time, which have nothing to do with school business.
• Finally, it has to be considered that the study and review were aimed at children in the 7th grade and entered into a context where interest was found in finding information about students' use of the equipment to watch porn.

• Considering these factors, the agency is of the opinion that the processing neither fulfilled the criterion of causality in section 5 (2) of the Act on processing of personal data, nor the proportionality requirement in section 5 (3), or the interest-weighting rule in section 6, 1, no. 7.

ESTONIA / ESTONIE

Major developments in the data protection field in Estonia 2016/2017

The annual report of the Estonian Data Protection Inspectorate for the year 2016 is available (in Estonian) at http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat_2016.pdf.
Summary of the annual report and recommendations from the Director General are available in English at http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/summary_annual_report_2016.pdf.

In the light of final adoption of the new EU data protection rules by the European Parliament in April 2016, Ministry of Justice disclosed a concept document of a Legal Framework for the Protection of Personal Data in April 2017. There is no intention to change the supervisory role of Estonian Data Protection Inspectorate. The document is available in Estonian at http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/andmekaitse_kontseptsioon_11.04.2017.pdf.

FINLAND / FINLANDE

The major developments in the data protection field in Finland in 2016

The biggest event of the Office of the Data Protection Ombudsman's 29th year in business was naturally the ratification of the new General Data Protection Regulation and the Data Protection Directive. We immediately set up an internal project to prepare for the new era. The Ministry of Justice appointed a multi-disciplinary working group to examine the effects of the data protection reform on our national legislation.

Data protection enquiries increase with digitalisation

Finland adopted a national data exchange layer in 2016. The objective of the new service is to give citizens safe access to the digital services of central government and local authorities. A high level of data protection has been one of the key priorities of the development project from the start. This involves taking the rights of special groups into account: Can these services still be accessed without digital devices as well? The administration also began a special project called DigiLeap. The Government has promised EUR 50 million towards increasing the population's digital skills. A project concerning the national Incomes Register also involved digitalisation.

Finland's new information security strategy is based on the premise that data protection and information security are national success factors that can also be turned into commercial services. These services are being conceptualised right now. The MyData concept, which has been the subject of much debate, is also in line with this ideology. Finland's national data system for healthcare services, which is called *Kanta*, and especially its *My Kanta* electronic portal for registered users gained popularity and promoted the transparency of data protection.

In today's increasingly digitalised world, guardians of law and fundamental human rights need to pull together. It is great that special legal delegates such as us have been able to build a horizontal partnership with the Human Rights Centre, the Chancellor of Justice and the Parliamentary Ombudsman.

The provision of social welfare and healthcare services is being reorganised across the country. Finland's regional government reform will bring with it major changes affecting controllers, for example. A working group on data management development has been set up to revamp data transmissions between public-sector controllers and the associated legislation.

Attention on open data, big data and banks' customer information questionnaires

Finland's national healthcare registers are an extremely popular subject for research scientists. Personal data protection is an important consideration in the fields of open data and big data, and the Office of the Data Protection Ombudsman has published guidance on this.

The finance sector's enquiries into their customers' relationships and background – which they must investigate by law – kept the Office of the Data Protection Ombudsman busy all year. My opinion is that the practical implementation of this EU-level requirement was poorly planned in Finland. Letters accusing consumers of copyright infringements also angered the public and resulted in a lot of work for us.

The highest Finnish courts, i.e. the Supreme Court and the Supreme Administrative Court, delivered several rulings with major implications on data protection in 2016. They related, for example, to registration offences, the publicity of documents, the disclosure of data from public authorities' personal data files, the use of personal data (patient records) in cases involving medical malpractice and electronic authentication.

Debate on the use of GPS tracking for road pricing and surveillance laws

The collection of road user charges on the basis of traffic data based on vehicle tracking upset the public due to its Big Brother-ish aspects. The project is now being reconsidered. On the other hand, work was

also in progress on a new surveillance law that would strip away much of the protection for confidential communication in particular. The project consists of four parts: amending the Constitution, laws on civilian and military surveillance and a proposal concerning the supervision of surveillance operations.

Finnish society also took a big leap forward in developing a national biobank and genetics strategy. Incorporating data protection into these concepts has proven very challenging.

The Office of the Data Protection Ombudsman has prepared itself for facing these major reforms. We have set up new projects, refined our communications and increased cooperation with our stakeholders. While all this was going on, we also handled almost 4,000 logged cases.

GEORGIA / GEORGIE

Office of the Personal Data Protection Inspector

INFORMATION ON MAJOR DEVELOPMENTS

(JUNE 2016 – JUNE 2017)

In 2016 the Office of the Personal Data Protection Inspector elaborated two major documents - Organizational Strategy (2017-2020) and two-year Action Plan (2017-2018). Promotion of the culture of respect to privacy and effective supervision are marked as the mission of the Office. In order to achieve its goals and objectives, DPA of Georgia carries out awareness raising campaigns/educational activities on a regular basis and expands its investigational activities.

Supervision

The Office of the Inspector carries out investigations either on the basis of citizens' complaints or on the Inspector's initiative. Inspections on the Inspector's initiative are mostly based on the risk analysis, which reveals the areas with large scale data processing and threats for privacy.

Throughout the reporting period, inspections were carried out both in private and public sector. In 2016, the Office carried out a total of 87 inspections. Public sector inspections *inter alia* included Prosecutor's Office, Ministry of Internal Affairs, Ministry of Probation, Revenue service of Georgia and municipalities. As per private sector, inspections were carried out in hospitals, universities, hotel chains, mobile and internet service providers, banks and other financial organizations.

Compared to the last year's statistics, the number of citizens' complaints and inspections doubled in 2016. The Office of the Inspector revealed 221 violations and imposed a fine on 63 organizations, while 35 institutions received a warning. Several public and private organizations were requested to apply appropriate organizational and technical measures in order to ensure data protection and 202 recommendations were issued for this purpose. Notably, the Office transferred 6 cases to the competent law-enforcement agencies due to presence of the elements of a crime.

It is also noteworthy that comparing to the previous years, in 2016 the number of consultations provided by the Office to citizens, public and private organizations increased three times.

Law-enforcement sector

Legislation related to the monitoring of covert investigational activities in the context of personal data protection was amended in 2017. By virtue of these amendments, the Inspector has the power to monitor all types of investigational activities carried out by police and prosecution service. Moreover, the Inspector monitors legitimacy of telephone communication interceptions and metadata access through electronic monitoring system.

Of notice, since June, 2016 the Office of the Inspector carried out inspections in 35 law enforcement agencies and handled 24 citizens' complaints against law-enforcement bodies.

Awareness raising and educational activities

The Office of the Inspector carries out large-scale information campaigns to inform the public on data protection rules, to promote data protection among data controllers and to involve civil society. Numerous trainings and public lectures were carried out. Free of charge trainings were available for representatives of data controllers. In addition, the trainings were also available for any individual interested in the issues of data protection, by registering on the official web page of the Office. Trainings for interested individuals are carried out on a monthly basis. During the reporting period, up to 700 representatives of private and public organizations were trained on data protection issues.

The office has recently implemented an awareness raising project - Data Protection Alphabet, which is aimed to spread knowledge on data protection among the population. The idea of the project is that behind each latter of the alphabet there is specific personal data, risks related to the data and possible ways to avoid these risks in an everyday life. The project delivers data protection basics to the public in an easily accessible language.

As per educational activities, Winter School on Data Protection was launched on January 28, 2017. Law and media students from 25 different universities of Georgia had an opportunity to acquire knowledge on data protection. In addition, The Office organized Data Protection Weekends for professors practicing in the field of media and law.

Other activities

- The Office of Personal Data Protection Inspector hosted the 19th meeting of Central and Eastern European Authorities.
- In December 2016, the meeting of Data Protection Authorities of Eastern Partnership Cooperation was held in Georgia.
- The Office of the personal Data Protection Inspector of Georgia, together with the representatives of public and private bodies, international and non-governmental organizations and academia organized National Internet Governance Forum in Georgia. Personal Data Protection and the Internet was one of the Panels of the National IGF.

GERMANY / ALLEMAGNE

Federal Republic of Germany: Major developments in the data protection field since June 2016

1. Profound reform of national data protection legislation with a view to the 2016 EU data protection reform package

In recent months the activities in the field of data protection almost completely focused on the challenging reform of the entire national data protection legislation following the far-reaching reform of EU data protection law in 2016. In May 2018, the EU General Data Protection Regulation (GDPR) will be applicable, and the Directive (EU) 2016/680 needs to be implemented by then. Therefore, there is an urgent need to bring national legislation in line with the new EU data protection rules. In May 2017, the German legislature adopted a profound reform of Federal data protection law, the so-called Act on the Alignment of Data Protection Law with the Regulation (EU) 2016/679 and on the Implementation of Directive (EU) 2016/680. The core element of the reform is a completely new Federal Data Protection Act. The next step will be the alignment of numerous federal laws containing specific data protection rules in various areas of law.

At the same time, all 16 federal states ("Länder") are preparing a profound reform of their respective data protection legislation in order to be compliant with the new EU data protection rules by May 2018.

2. Amendment of the Federal Data Protection Act concerning video surveillance

On 5 May 2017 the modified provision on video surveillance (§ 6b of the Federal Data Protection Act) entered into force. This modified provision further specifies the relevant criteria for the assessment of the legality of video surveillance by private controllers in large-scale facilities open to the public (e.g. shopping malls, parking lots etc.) as well as in the public transport system. The provision clarifies that in these places the protection of life, health and freedom of human beings must be particularly taken into account when deciding whether or not video surveillance is in line with the right to privacy.

ICELAND / ISLANDE

Information on Major Developments in the Data Protection Field
June 2016 – May 2017

The Icelandic Data Protection Authority
At the moment, six people work at the Icelandic Data Protection Authority, including four lawyers, an office manager and the Data Protection Commissioner, Ms Helga Þórisdóttir. The Ministry of the Interior appointed a new Board of Directors of the DPA on 30 June 2016. Chairman of the board is Ms Björg Thorarensen.

General Data Protection Regulation (GDPR)
The Ministry of the Interior 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 is participating in the working group.

The DPA‘s requests for a significant budget increase due to the implementation of the GDPR have not yet been met. Updated proposals have been presented to the Ministry of the Interior (now the Ministry of Judicial Affairs), to the Budget Committee and the Judicial Affairs and Education Committee of the Icelandic Parliament, Alþingi. A final decision on this matter has not yet been taken.

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

European Data Protection Day – 28 January 2017
An interview with the Data Protection Commissioner, Ms Helga Þórisdóttir, was published in Morgunblaðið (The Morning Paper) on 26 January. This edition of the newspaper was distributed into every home in Iceland. On Data Protection Day, 28 January, a follow-up article, written by Ms Þórisdottir, was published in the same newspaper. The interview and the article focused on Data Protection Day, the new General Data Protection Regulation, and the importance of data protection in the information age.

UT-messan – 3-4 February 2016
UT-messan is one of the largest IT events in Iceland. 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 DPA‘s Head of Audit and Security gave a presentation on Data Protection and Artificial Intelligence.

GDPR Seminar – 30 September 2016
On 30 September 2016, the DPA held a seminar on the new GDPR at Reykjavik Hotel Natura. This event was open to the general public and was attended by over 300 people.

Other events
The DPA has given lectures and presentations on GDPR and other data protection-related subjects on 15-20 occasions in the past year, including the Government‘s IT day, The Internal Auditing Day, and a meeting with directors within ministries and public organisations.

Media Coverage
Data protection has been an increasingly popular subject with the Icelandic media lately. The DPA‘s rulings are frequently reported and the Data Protection Commissioner has been interviewed on multiple data protection-related subjects in newspapers, radio and television.

Statistical Data
According to statistical data, during 2016 the DPA received a total of 1.865 new cases, including 99 formal complaints, 479 inquiries, 495 notifications on the processing of personal data, 28 inspections and 309 cases related to scientific research within the health sector. Other projects include reviews on parliamentary bills and ministry regulations, consultations, opinions, lectures 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 2016, will be available soon at the DPA's website, www.personuvernd.is (in Icelandic only).

IRELAND / IRLANDE

Report from Ireland on Major Developments (June 2017)

A key focus of developments in the data protection field over the last year has been preparation for the coming into operation of the General Data Regulation [Regulation (EU) 2016/679] and the law enforcement Directive [Directive (EU) 2016/680] in May 2018.

Data Summit, June 15 and 16 2017, Dublin
The Data Summit which takes place on 15 and 16 June 2017 will be a major, two day international conference bringing together a range of stakeholders to consider and highlight some of the issues arising from the ever expanding role of data in modern life.

A range of international, European and national speakers from a range of disciplines and backgrounds will deliver a mix of keynote addresses, panel sessions and workshops covering key topics, including:

- Maximising the potential of data driven technologies for our society and economy;
- Achieving the right balance around privacy and personal data, security and innovation;
- Practical steps to prepare for the General Data Protection Regulation;
- How people can manage their own privacy in an online world;
- Showcasing developments and best practice around positive innovation and societal benefits arising from the good use of data.

The overall aim is to stimulate two days of conversations about data issues among a broad audience from enterprise, academia, government, civil society and the general public.

Publication of Draft Data Protection Bill
The draft Data Protection Bill 2017 was published in May. The Bill gives further effect to the GDPR; transposes the law enforcement Directive into national law; and replaces the Data Protection Commissioner with a Data Protection Commission with the possibility of up to three Commissioners depending on future workload.

Office of Data Protection Commissioner

Budget and Organisation
The budget of the Office of the Data Protection Commissioner (DPC) increased from €4.7 million in 2016 to €7.5 million in 2017, facilitating an expansion in staff including legal, investigative, business analysis, and communications staff. By the end 2017, the DPC will have almost 100 staff.

In addition to the Office's location in Portarlington, the DPC established a Dublin base in autumn of 2016, formally opened by An Taoiseach Enda Kenny, T.D., in January 2017.

2016 was the first full year of the operation of the DPC's Special Investigations Unit. This Unit carries out investigations on its own initiative, rather than investigations based on complaints. It is currently conducting ongoing investigations into the private investigator sector, and the hospitals sector in respect of how patient files and data are managed in areas accessed by patients and the public.

In 2016 the DPC established a new Multinationals and Technology team in order to coordinate regulatory activities in this area. 2016 also saw the establishment of a centralised legal unit within the office.

GDPR Awareness Raising
The DPC is utilising a number of communications channels to raise awareness of the GDPR, and publish and disseminate guidance materials on preparing for compliance with the new Regulation.

In October 2016 the office's Twitter account was established and on 25 May 2017 a new website www.GDPRandYOU.ie was launched to raise awareness of the GDPR.

The DPC also continues to raise awareness with stakeholders through speaking and presenting at seminars, conferences, and to individual organisations.

2016 Annual Report
The 2016 Annual Report of the Data Protection Commissioner was published in April. The Report highlights key developments and activities of the Office in 2016, together with priorities for 2017 and beyond. The Report is available at www.dataprotection.ie.

ITALY / ITALIE

Major developments in the data protection field

ITALY

(June 2016 - June 2017)

Data Protection Law

From June 2016 to June 2017 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).
The Italian DPA (Garante per la protezione dei dati personali, henceforth "Garante") has nevertheless followed the legislative process of a number of legislative decrees and laws which, although not amending the Data Protection Code, had impact on data protection.
It is to be signalled that Law no 71 of 29 May 2017 on cyberbullying have given new tasks to the Italian DPA which is now competent for requests for deletion and block of data related to minors which have been unlawfully processed for the purpose of cyberbullying.

Main activities of the Data Protection Authority

(All the decisions mentioned below can be found on the Italian DPA web site www.garanteprivacy.it)

June 2016
Data processing for fraud detection
A prior checking request was rejected by the Garante concerning the project of a company in the car rental sector to create a centralized database aimed at contrasting frauds related to rented cars. The intention of the company to include in the data base personal data of clients (including judicial data) was deemed to be not proportionate to the aim pursued.

Right to be forgotten
A decision by the Italian DPA denied to an ex-terrorist the delisting from search engines of news concerning his crimes. In this decision such news was still actual and the crimes committed had relevant repercussions on the society and even on the history of Italy. The conclusions may have been different if, for example, the request concerned a crime committed many years before but with no persistent relevance for the public opinion. In that case the right to be forgotten and to "renew" the person's identity could have prevailed.

Code for digital administration

The Garante adopted an opinion on the draft legislative decree containing amendments to the Code for digital administration where the need for more stringent safeguards for individuals' privacy was signalled.

Profiling in insurance sector

The Garante adopted a decision, under a prior checking request, regarding the intention of an insurance company to use an application aimed at monitoring driving behaviors of their clients. The decision underlined that such project would be legitimate only after having adequately informed the clients, provided limited data retention periods, and adopted adequate safeguards for ensuring the right to the protection of personal data.

July 2016

Internet banking

A prior checking was submitted to the Garante for the assessment of a project aimed at detecting fraud in internet banking based on the analysis of behavioral and biometric data related to users. The Garante acknowledged the legitimate purpose of fraud detection but it conditioned the start of the project to the adoption of appropriate measures for protecting users' data protection.

Employment sector: monitoring of employees

Indiscriminate controls on employees' e-mail and on their use of Internet, according to a decision of the Italian DPA, are in contrast with the Data Protection Code and the Statute of workers. Against this background, the Garante banned the monitoring carried out by a university on its employees. In such decision the DPA highlighted that the university should have opted for gradual measures that would render controls residual and not massive.

Apps for employees' smartphones

Again in the employment sector, the Garante adopted a decision regarding the project of two companies which intended to install an application on their employees' smartphones to detect the time of the start and end of their work activity. The Authority ordered the two companies to adopt the system by using a privacy by design approach, therefore limiting the processed data to those strictly necessary and to ensure the accuracy of the data.

On line petitions

The Garante started an investigation on Charge.org Inc, the international platform for on line petitions. The intervention of the Garante aimed at assessing the modalities of the processing of data related to those who sign to promote or adhere to petitions, which may reveal sensitive information, also with regard to possible profiling based on the collected information.

August 2016

On line publication of data

The Garante banned the publication on the website of a regional administration of data related to (thousands) individuals who had applied for – and not obtained - public contributions, and who were in economic discomfort. The publication was carried out in the absence of appropriate legal basis.

September 2016

Privacy Sweep

The Italian DPA participated in Privacy Sweep 2016 promoted by the Global Privacy Enforcement Network (GPEN) to assess the respect for data protection standards in the sector of the Internet of things. From the joint assessment emerged that in such field the level of awareness regarding the importance of data protection rules is not sufficient.

Cooperation with DPAs

The Garante continued its cooperation with other data protection authorities. In September 2016 a memorandum was signed with the Moldavian DPA aimed at promoting cooperation between the two authorities.

Whatsapp

The Garante started an investigation on the processing carried out by Whatsapp in particular in respect of the modifications to their Privacy policy which provided the communication of data related to users' accounts to Facebook also for marketing purposes.

October 2016

Code of Ethics and Conduct in Processing Personal Data for Business Information Purposes

The Code of conduct for the processing of personal data for business information purpose (As published in Italy's Official Journal No. 238 of 13 October 2015) entered into force on the 1st of October 2016.
The code, which was promoted by the Garante, and is now attached to the Data Protection Code, sets forth safeguards to ensure that the collection and use of data for business purpose is carried out with due respect for the right to privacy and the protection of personal data. According to Article 12 of the DPCode, the respect for the principles contained in the code is a pre-requisite for the processing to be legitimate

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5483022

November 2016

Reputational profiles

The DPA prohibited the processing related to a web platform aimed at elaborating- by means of algorithm – reputational profiles on the basis of the collection from various sources including the Internet. Such decision was based, amongst others, on the absence of sufficient security measures and of transparency requirements, prolonged data retention periods, and the relevant impact on the individuals of the attributed rating.

Privacy Shield

The DPA adopted the authorization for data transfers to the United States on the basis of the Privacy Shield agreement which was signed by US and EU. The authorization replaces the previous one, which regulated such flows of data in the light of the Safe Harbor agreement which has been invalidated by the European Court of Justice. The Italian DPA has reserved the possibility to verify the lawfulness and fairness of the transfer of data and to adopt, if necessary, the measures provided for by the Data Protection Code.

January 2017

Telemarketing

The Garante prohibited the processing of personal data collected on the Internet for telemarketing purposes without the informed data subjects' consent. The decision restated that the fact that users' phone numbers are available on line does not mean that they can be unlawfully used for purposes which are different from the ones that justified their publication.

February 2017

Online publication of judicial data

The DPA ordered to Yahoo! Emea Limited the deletion of the link to a US website which published daily arrests occurring in the United States and where inaccurate information was published concerning an Italian citizen involved in a judicial case that occur in the US.

Publication of data related to a minor on social network

The Garante ordered a woman to remove from her Facebook page two sentences, on the cessation of the civil effects of marriage, where delicate aspects of family life were reported, including the minor daughter.

March 2017

Money Transfer

The Italian DPA sanctioned five companies working in the money transfer sector for a total of 11 Millions of euros for unlawful processing of personal data. The processing in question was carried out without the data subject's consent and in some cases the forms for the transfer were completed by inexistent individuals or not signed.

National DNA database

The Garante issued its positive opinion on the draft of the last implementing decree that regulate the national DNA database. However, the Authority has called for greater safeguards regarding the updating of data, the deletion of those referring to persons acquitted by final judgment and clear requirements for the access to information by national institutions.

June 2017

Joint sector inquiry on Big data

In June 2017 the Garante together with the Italian Competition Authority and the Communications Authority opened a joint sector inquiry on "Big data", aimed at identifying potential concerns and defining a regulatory framework able to foster competition in the markets of the digital economy, to protect privacy and consumers, and to promote pluralism within the digital ecosystem.

* * *

EU reform package

In view of the application of the new EU Data Protection Regulation, our Authority in the course of the year has launched initiatives aimed at providing both private and public actors with guidance for facilitating the compliance with the new rules.

http://www.garanteprivacy.it/regolamentoue

LATVIA / LETTONIE

Data State Inspectorate of Latvia (hereinafter – Inspectorate) has received Secretariat of Council of Europe e-mail letter of 27th April, 2017 *(registered in Inspectorate with No.7-4.3/105-S)* concerning major developments in the data protection field since the last plenary meeting held in June 2016.

In response to your request, Inspectorate hereby would like to inform that since the last plenary meeting held in June 2016 an ongoing active work on structural changes of Inspectorate is carried out in order to effectively prepare for General Data Protection Regulation. Simultaneously Inspectorate informs that considerable work is ongoing to strengthen the independence of Inspectorate.

Inspectorate would like to express the gratitude for your kind cooperation.

Data State inspectorate of Latvia

LITHUANIA / LITHUANIE

34 PLENARY MEETING OF THE COMMITTEE THE CONVENTION 108
STRASBOURG, 19 – 21 JUNE, 2017
COUNTRY REPORT – LITHUANIA

1. Recent National Developments – legal framework

1.1. As regards drafting of the laws the priority is given to preparing for the application of the new legislation on the protection of personal data of the European Union.

1.2. The Code of Administrative Offences of the Republic of Lithuania entered into force since 1st January 2017

The new Code of Administrative Offences of the Republic of Lithuania that entered into force from 1st January 2017 and replaced the Code of Administrative Offences of the Republic of Lithuania approved in year 1984.

According to the provisions of the new Code penalties for offences relating to the protection of personal data have been increased.

The lowest fines the natural person shall pay for violation of any of these laws, Law on Legal Protection of Personal Data, the Law on Electronic Communications or Cyber Security Law are 150 EUR to the natural person and 300 EUR to the legal entity or other responsible person and the highest – 1200 EUR and 3000 EUR accordingly.

Also according to the new Code of Administrative Offences the SDPI is entitled to decide on sanctions.

1.3. Changes of the Law on Electronic Communications of the Republic of Lithuania

Having regard to the Judgment of the European Court of Justice in the Joined Cases C-203/15 and C-698/15 changes of the Law on Electronic Communications of the Republic of Lithuania related to the use of traffic data and issues of data retention have been drafted and now are under discussions of SEIMAS (the Parliament of the Republic of Lithuania).

2. Case law

2.1. The State Data Protection Inspectorate (hereinafter - SDPI received a person's which was a defendant complaint, which stated that the advocate which represent the plaintiff (not the applicant) disclosed in writing data of civil case (hearing was in close session) to a head of certain state institution which was not related to the civil case. The advocate sent a request, which provided the following information: "District Court investigates civil case No <...> according to the claim of plaintiff (initials) on <nature of the case>." The SDPI recognized the applicant's – defendant's complaint well-founded and wrote a protocol on administrative offense to the advocate, as advocate by sending a request to the head of certain state institution, unlawfully disclosed the applicant's personal data of the case against her and the nature of case to a head of certain state institution. The Court of First Instance terminated proceeding of case of administrative offences against advocate.

SDPI appealed court decision and the advocate has been found guilty by the court of Second Instance of the Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter – the LLPPD) and the court fined him.

The advocate appealed this court decision to the Lithuanian Supreme Court with a request for a case of administrative offence to be reopened.

According to the case material Lithuanian Supreme Court founded that the advocate, as a representative of plaintiff in a civil case, sent a request to the head of certain state institution, which provided the following information: "District Court investigates civil case No <...> according to the claim of plaintiff (initials) on <nature of the case>."

Judicial panel concluded that the information provided by the advocate to a third person (head of the state institution), that there is a civil case pending at court under the claim of plaintiff against the defendant on <nature of the case>, is disclosure of the applicant's personal data and information about a person's private life (name, surname, name and surname of their spouse's, situation in the family (information that the court investigates civil case for divorce)) and information describing the applicant (information that the marriage is terminated due to his fault) transmitted or otherwise made available.

Paragraph 1 of Article 27 of the LLPPD provides that, in the cases referred to in subparagraphs 5 and 6 of paragraph 1 of Article 5 of this Law, the data controller must inform a data subject about his right to object to the processing of his personal data. This means that the advocate could indicate the applicant's personal data to a third party only if he has his consent and such consent has not been obtained.
Judicial Panel found that the advocate undoubtedly violated the LLPPD.

2.2. The SDPI having received information on a possibly unlawful CJSC "T" direct marketing to CJSC "W" and consequently possible violation of the paragraph 1 of Article 69 of the Law on Electronic Communications (hereinafter – the LEC), carried out an investigation on its own initiative. During the investigation it was determined that the CJSC "T" without having prior consent of CJSC "W" used for direct marketing purposes CJSC "W" publicly published telephone number – offered to buy CJSC "T" goods. Due to that the SDPI issued for CJSC "T" order to ensure that electronic communications services for direct marketing purposes to be used only having obtained a prior consent of the subscriber, including use of a publicly available telephone numbers (hereinafter – Order).
CJSC "T" appealed the Order to the Vilnius Regional Administrative Court, stating that definition of "direct marketing" shall be interpreted and applied according to the aim of the LLPPD – to safeguard of the inviolability of an individual's private life in the course of processing personal data. Accordingly, direct marketing shall be related only to private natural person, because the application of the same requirements to a legal person as to the natural person would misrepresent the essence and objectives of a legal regulation.
Vilnius Regional Administrative Court decided to abolish the Order stating that in view of the key objectives of the SDPI – supervision and control of personal data processing activities – it could be said that the SDPI is empowered to supervise and control the provisions of the LEC only related to the protection of personal data processing which in accordance with definition provided in the paragraph 1 of Article 2 of the LLPPD shall be related only to the natural, rather than a legal person, processing.
The Lithuanian Supreme Administrative Court having reviewed the case by the appeal of the SDPI concluded that the SDPI powers in the paragraph 12(1) of Article 5 of the LEC are not differentiated dependently on the type of subject – natural or legal person, to whom provisions of the LEC shall be applicable. The Lithuanian Supreme Administrative Court stated that deciding on the question of applicability of the Ninth Section of the LEC to a certain range of subjects there is no legal ground to follow provisions of the LLPPD because legal nature of relations regulated by these legal acts is not the same. The Lithuanian Supreme Administrative Court drew attention to the fact that the paragraph 12(1) of Article 5 of the LEC by referring to the LLPPD indicates a procedural aspect – notes that the SDPI in accordance with the LLPPD exercises powers granted ("...in accordance with the LLPPD investigates complaints on processing of personal data and privacy protection ..."). The Court stated that under the paragraph 1 of Article 69 of the LEC use of electronic communications services, including e-mail messaging for direct marketing purposes is permitted only with the prior consent of a subscriber or registered user of electronic communications services. Paragraph 1 of Article 3 of the LEC states that the subscriber shall mean any person who or which is party to a contract for the provision of public electronic communications services with the provider of such services. Provisions of the LEC separates user (paragraph 3 of Article 69 of the LEC), which are considered a natural person. Thus, having evaluated Paragraph 1 of the Article 3 of the LEC the Lithuanian Supreme Administrative Court has decided that there is no legal ground to assert that definition of the subscriber established in this paragraph includes only natural persons. Vilnius Regional Administrative Court decision was annulled.

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

2.4. A person lodged a complaint because the State Tax Inspectorate disclosed his personal data about tax inspection that was still in process to media. According to paragraph 1 of Article 38 of the Law on Tax Administration of the Republic of Lithuania the tax administrator shall keep Information on tax payer confidential and use it only for lawful purposes. According to subparagraph 6 of paragraph 2 of Article 38 of this law information relating to tax violations shall not be kept confidential if the taxpayer's fault for tax law violations is proven. The SDPI decided that the State Tax Inspectorate disclosed personal data of the complainant about the tax inspection that was started but was not completed at that time yet illegally, not having any legal ground provided for in Article 5 of the LLPPD or any other criteria for lawful disclosure of personal data. The SDPI gave an instruction to the State Tax Inspectorate not to use the former practice to inform media (according to requests of the media) about tax inspections of natural persons while they are still in process because the taxpayer's fault for tax law violations is not proven yet.
This instruction was appealed to the Vilnius District Administrative Court by the State Tax Inspectorate pleading that disclosing the fact of a started tax inspection is one of the means to prevent violations and giving information about the activity of the institution. The Court dismissed the appeal, founding on Article 38 of the Law on Tax Administration and stated that disclosure of taxpayer's personal data could not be justified by the aim to prevent violations and to give information about the activity of the institution.
The State Tax Inspectorate appealed this decision to the Supreme Administrative Court, which also dismissed the appeal.

MALTA / MALTE

Major Developments in the Data Protection Field covering 2015 and 2016

A. Summary of activities and news

As in previous years, during the period under review the Office of the Information and Data Protection Commissioner maintained the proactive approach of meeting the various sectors within the local indutry with the firm objective to discuss their business operations and address any arising data protection issues or concerns which would necessitate an intervention by the Commissioner. This Office adopts an approach whereby it coordinates such meetings with the wide representation of the respective sector. This approach proves to deliver satisfactory results particularly where guidelines or codes of practice would need to be developed in order to regulate specific areas within the sector.

During this period this Office continued its internal review exercises designed to implement the Government's overarching policy to ensure better regulation. Furthermore the Office honoured its European and international commitments by participating in various data protection fora.

Awareness raising activities were carried out by this Office during the period under review which included the delivery of presentations to various data controllers in different sectors of the Maltese economy, participation in local TV and radio programmes with phone-ins and the regular updating of the Office's portal (www.idpc.gov.mt) with developments occurring in the field of data protection. This Office firmly believes that getting the message across via the media, represents a potential and effective way to increase awareness with the public at large.

B. Statistics for 2015 and 2016

Apart from information on the data protection field, this section provides information on the implementation of the Freedom of Information Act (which also falls within the remit of the Office of the Information and Data Protection Commissioner)

	2015	2016
Total number of official Data Protection Complaints	64	58
- Right of access	2	6
- CCTV cameras	8	10
- Unauthorised disclosure	3	4
- Unsolicited communications for marketing purposes	17	12
- Unlawful processing	34	26
Breaches of the Data Protection Act	31	15
Number of fines imposed on data controllers	5	1
Appeals lodged challenging data protection decisions	5	6
Freedom of Information complaints	8	21
Freedom of Information decisions where the Public Authority was found to have dealt with a request not in accordance with the Freedom of Information Act	4	6
Number of fines imposed on Public Authorities	1	0
Appeals lodged challenging Freedom of Information decisions	1	3
Appeals lodged by the Information and Data Protection Commissioner challenging the Information and Data Protection Appeals Tribunal's decisions:	0	0
- Data Protection	0	0
- Freedom of Information	0	0
Total number of prior checking requests:	37	18
- Education sector	13	5
- Health sector	8	5
- Financial sector	3	0
- Government departments and entities	10	7
- Others	3	1
Data breaches reported	0	2 (not from telcos)
Authorisations for transfers to third countries	1	2
New notifications forms	251	192

MAURITIUS / MAURICE

The Data Protection Office of Mauritius (DPO)

The Data Protection Office has witnessed a tremendous leap in the achievement of its objectives as data protection has substantially and positively grown in stature and influence. As a privacy authority, the DPO has persevered in diversifying its services through sensitisation, training, publication of guidelines, registration of data controllers, issuing notices to data controllers, investigation on complaints, compliance audits, authorisation for transfers of personal data abroad and providing timely advice to organisations on data protection.

The major developments in the data protection field since June 2016 till date are:

- The ratification of Mauritius in June 2016 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as "Convention 108". This has been instrumental in strengthening the data protection legal framework in Mauritius with international best practices and is a huge thrust forward for the country as the second non-European state after Uruguay and the first country in Africa to ratify this convention. One amongst the advantages derived as being a party to the Convention is that Mauritius is considered a country with a safe flow of data to attract foreign investment.

- The Data Protection Commissioner (DPC) has provided 14 decisions after successful complaint investigation pertaining to:
    - Usage of CCTV cameras
    - Illegal appropriation of fingerprints and biometric attendance
    - Disclosure of information
    - Excessive Information
    - Unsolicited promotional SMS messages

  A summary of the decisions is available on the website of the office at the following link: http://dataprotection.govmu.org/English/Pages/Decisions-on-Complaints.aspx. The decisions of the Data Protection Commissioner are appealable at the ICT Appeal Tribunal of Mauritius and no appeal has been registered against the above decisions.

- Continuons collaboration with international counterparts such as Association Francophone des Autorités de Protection des Données Personelles (AFAPDP), Réseau Africain des Autorités de Protection des Données Personelles (RAAPDP), Commission Nationale de l'Informatique et des Libertés (CNIL) France, Global Privacy Enforcement Network (GPEN), Common Thread Network (CTN) and sharing of information, experiences and best practices.

- The office launched a Privacy Compliance Assessment Web Application Tool on its website to help organisations assess their compliance with the Data Protection Act 2004 in order to proactively identify and avoid privacy breaches.

- The implementation of a new e-service system for online registration and payment of data controllers and submission of online complaints. The back office of the system is already operational.

POLAND / POLOGNE

Country report on major developments in the data protection field

I. Legislation

1. Recent National Developments – legal framework

On 7 October 2016 the Act on trust services and electronic identification entered into force. The Act repeals the existing legal provisions in this regard on electronic signature and introduces the provisions of the eIDAS Regulation to be applied. In particular, the Act modifies 82 acts as regards the issues of identification and electronic signature, including the Code of Administrative Proceedings, the Act on providing services by electronic means and the Act on informatisation of entities performing public tasks.

On 2 July 2016 the Anti-terrorism Act entered into force, which – despite of GIODO's objection – introduced registration of prepaid cards and grounds for collection of materials from operational activities without regulation of the storage period. The principles of exercising supervision over activities carried out in relation to suspected persons also raised GIODO's doubts. The Act sets forth that decision on monitoring suspected persons and carrying out operational activities shall be taken by the Public Prosecutor General without notifying the court. Moreover, the Act provides for keeping a list of persons who may be related to terrorism, without specifying the scope of information contained on the list as well as its storage period, which was requested by GIODO. GIODO raised also objections concerning the right to block access to ICT services, requesting their further specification and the possibility to appeal from the decision in this regard to the court. The comments presented by GIODO were not taken into account.

On 21 October 2016 the Sejm of the Republic of Poland (lower chamber of the Polish Parliament) adopted the Act on the national tax administration, which modifies tax administration organisation. In GIODO's view the Act entitles tax authorities to non-defined scope of personal data processing. The Act does not indicate the scope nor the period of storage of the data collected from tax payers. At the stage of legislative works, GIODO drew attention to incompliance of proposed provisions with the currently binding Act on Personal Data Protection and with the General Data Protection Regulation by the Parliament and by the Council. Those opinions were not considered.

II. Ahead of the EU data protection reform

On 27 June 2016 GIODO appointed the Experts Commission for the reform of personal data protection in the EU, including next to GIODO's experts also experts from various milieus, e.g. DPOs. Its task is to analyse essential legislative changes in the Polish legal system in connection with the entry into force of the GDPR. The Commission will also draw up opinions and studies on specific solutions adopted in the GDPR.

On 8 July 2016 the Polish DPA appointed from among its employees the Team for Personal Data Protection Reform in the EU.

Within the framework of preparations for the implementation of the new EU data protection framework, GIODO has been undertaking a variety of educational activities for the purpose of increasing awareness of both data subjects and Data Protection Officers, including for example conferences, trainings, workshops etc. (see point III Events below). Also, the experts from the Polish DPA developed a Guide for DPOs "Performance of DPOs Duties in the Light of the General Data Protection Regulation". Moreover, GIODO drew up a set of questions which are to help the data controllers to evaluate the state of their preparation for the application of the new law.

III. Events

On 7 December 2016 in Warsaw a **Poland-wide Conference entitled "Implementation of the General Data Protection Regulation – Procedural Aspects"** was organised by GIODO, the President of the Supreme Administrative Court and the Dean of the Faculty of Law and Administration of the University of Warsaw. The event was attended by over 200 persons representing administrative courts, public administration, as well as academics and entrepreneurs. The conference focused on selected topical issues which required discussion before commencing the application of the GDPR.

Moreover, in 2016 GIODO launched a series of **trainings for Data Protection Officers** (DPOs) from selected sectors. In 2016 the Polish DPA carried out 2 trainings for DPOs from the public sector (28 June and 9 September 2016) and the higher education sector (24 November 2016). In 2017 GIODO conducted 2 trainings for DPOs from the medical sector (1 and 2 March 2017) and a training for DPOs from the Polish courts (23 May 2017).

In 2017, just like in previous years, GIODO celebrated, already for the 11th time, the **European Data Protection Day**. As each year, conferences devoted to most recent issues related to the right to privacy and data protection are held, including:

31 January 2017, Warsaw – the Conference on Personal Data Protection in the Era of Changes organised by GIODO. The possibility to obtain legal advice on personal data protection provided by GIODO's representatives.

3 February 2017, Dąbrowa Górnicza – Open Day of the Inspector General for Personal Data Protection organised by the University of Dąbrowa Górnicza at its premises in cooperation with GIODO.

Furthermore, in **January/February 2017** 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.

On 23 March 2017 in Krakow GIODO organised the subsequent **Meeting of DPAs from the Visegrad Group Countries**, focused mainly on discussing and exchanging experiences related to the application of the General Data Protection Regulation, having in mind proper preparation of DPAs for new challenges.

IV. GIODO projects and programmes

Within its educational activity, GIODO is inter alia involved in realising EU co-funded projects. In the reporting period the Polish DPA continued implementation of the project co-funded by the Fundamental Rights and Citizenship Programme of the EU - 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.

The subsequent PHAEDRA II Project Workshop was organised by GIODO on 18 October 2016 in Marrakech, within the framework of the 38th International Conference of Data Protection and Privacy Commissioners. It was devoted to cooperation of European Data Protection Authorities from the perspective of „trust".

Moreover, GIODO is one of the partners of a project funded by the European Commission **Erasmus+** "Key Action - Cooperation for Innovation and the Exchange of Good Practices, Action - Strategic Partnerships for Higher Education". The realised project is aimed at developing an innovative programme of postgraduate studies regarding personal data protection, which would meet market needs. The coordinator of the project is the University for Information Science and Technology St. Paul the Apostle, Ohrid (Macedonia) and the partners of the project are the Inspector General for Personal Data Protection (Poland), the Directorate for Personal Data Protection (Macedonia), the Commission for Personal Data Protection (Bulgaria) and the University of Lodz (Poland). The project shall be realised within 28 months.

V. Agreements on cooperation

In the reporting period GIODO concluded agreements on cooperation on the protection of privacy and personal data with a dozen or so institutions, including inter alia the banking, insurance and Internet sector, universities, the Supreme Administrative Court, the Ombudsman for Children and the Polish Chamber of Information Technology and Telecommunications.

MEXICO / MEXIQUE

MAJOR DEVELOPMENTS IN THE FIELD OF DATA PROTECTION FROM JUNE 2016 TO MAY 2017 NATIONAL INSTITUTE FOR TRANSPARENCY, ACCESS TO INFORMATION AND PERSONAL DATA PROTECTION (INAI-MEXICO)

1. Guide for the secure deletion of personal data

On July 2016, the Institute launched a document to guide data controllers on the general criteria for the destruction, elimination and safe deletion of personal data. The Guide is available at: www.inai.org.mx

2. 46° Asia Pacific Privacy Authorities (APPA) Forum

The 46° APPA Forum was hosted by the National Institute for Transparency, Access to Information and Personal Data Protection (INAI-Mexico) on 30 November - 2 December 2016 in Manzanillo, Colima. During the two-day forum, APPA members, invited observers and guests discussed a range of matters including: cross-border data transfers, international cooperation, self-regulation schemes, effective dispute resolution mechanisms, law enforcement, among others.

The event was attended by representatives of the data protection authorities of Australia, British Columbia, Canada, Colombia, Japan, South Korea, New Zealand, Philippines, Singapore, United States, Victoria, Hong Kong and Macao. Also attending were representatives from the United Nations, the National Commission for Information Technology and Civil Liberties of France, the Spanish Data Protection Agency and the UK Information Commissioner's Office.

3. Visit of Joseph Cannataci, UN Special Rapporteur on the right to privacy

Joseph Cannataci, UN Special Rapporteur on the right to privacy, was the keynote speaker at the 46° APPA. During his intervention, he highlighted that privacy is more than a material good, it is a universal and fundamental human right.

During his visit to Mexico, Professor Cannataci held several meetings with the Federal Police and the Federal Judiciary Council; Organizations of the Civil Society; and with organizations that work with indigenous communities.

4. Data Protection Day 2017

The Institute organized a one-day event attended by 700 people that was divided into an opening ceremony, one keynote speech given by Trevor Hughes (President and CEO of the International Association of Privacy Professionals), two panels on the protection of personal data of the Digital Citizen in the public management and the challenges of the protection of personal data of the digital consumer. The agenda also included an award ceremony of two competitions: “Prize of Innovation and Good Practices in the Protection of Personal Data” and “Urban Art and neo-muralism contest: Art is Public; your personal data is not”.

The Institute also organized one-day conferences and panels in 7 cities throughout the country in order to promote a data protection culture.

5. Prize of Innovation and Good Practices in the Protection of Personal Data (first edition)

The competition had the following objectives: to identify, to know and to spread, at national and international level, the best practices on personal data protection; to create positive incentives for the development and promotion of initiatives and practices on personal data protection; to encourage and strengthen the exercise of the rights of access, rectification, cancellation and opposition; and to promote the improvement of the procedures used in Mexico by data controllers and data processors

6. General Law on Protection of Personal Data Held by Obligated Parties

On January 26, 2017, the General Law on Protection of Personal Data Held by Obligated Parties (LGPDPPSO) was published in the Mexico’s Federal Official Gazette. The main purpose of this General Law is to establish, in the federal, state and local sphere, the bases, principles and procedures required to uphold the right of any person to the protection of his/her personal data held by any authority, entity, agency or body of the Executive, Legislative and Judiciary Branches, autonomous entities, political parties, trusts and public funds.

The General Law ratifies Mexico's commitment to work with a human rights perspective for the benefit of its population and, at the same time, Mexico is inserted in the list of countries that contemplate a wide and innovative regulation on this matter.

7. **Ibero-American Data Protection Standards**

It is a project developed by the Ibero-American Data Protection Network. The Standards would be guidelines addressed to the data protection community, specially to those Ibero-American countries that are developing their own privacy legislation.

Standards are expected to be approved during the XV Ibero-American Data Protection Meeting that will take place in Santiago de Chile, Chile, on June 2017.

8. Jurisprudence Platform "Corpus Iuris on personal data protection"

The "Corpus Iuris" is the first database in the Ibero-American region that groups different documents on personal data protection, privacy, intimacy, private life, habeas data, and other related issues.

The database comprises international treaties and international conventions, resolutions issued by jurisdictional bodies, criteria of quasi-jurisdictional bodies, criteria derived from reports from around 28 regional and international organizations.

Mexico launched the platform within the framework of the XIV Ibero-American Data Protection Meeting, held on June, 2016.

9. Ibero-American Data Protection Classroom

It is an academic online course on data protection and privacy addressed to undergraduate students.

In Mexico, the project started as an optional course taken by 400 Law students of the Faculty of Law and Social Sciences of the Benemérita Autonomous University of Puebla.

Currently, the Ibero-American Data Protection Classroom has expanded its coverage in Mexico to 5 other Universities and it is available for any Spanish-speaking University.

REPUBLIC OF MOLDOVA / REPUBLIQUE DE MOLDOVA

Major developments in personal data protection

in the Republic of Moldova for 2016

During 2016, the personal data protection field in the Republic of Moldova has experienced several major developments.

1 – Two drat laws proposed

The first major development was the drafting of two new laws regarding personal data protection in the Republic of Moldova. These laws aimed to enhance the current national legal framework in this field.

The first text - *Draft law amending and supplementing certain legislative acts* (including Law on personal data protection) - looks to enhance the functional and operational capacities of the Center to intervene with adequate responses to the breaches committed by personal data controllers in the context of personal data filling systems security incidents. It aims as well to enables the National Center for Personal Data Protection (NCPDP) to perform checks on the lawfulness of personal data processing in areas not falling expressly within the scope of current law. Finally, this draft will contribute to the fulfilment of the commitments undertaken in relation to the European Union.

The second draft law - the *Draft Law on the National Center for Personal Data Protection* - focuses on strengthening the capacity of the NCPDP as an institution. Thus, it provides an increase of the staff-limit from 21 to 45 employees, an increase of the nature and amount of the pecuniary sanctions, clarifies the control procedure and provides legal protection of the institution's employees.

The Council of Europe's experts gave a positive opinion concerning both laws in term of compliance with the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows. The expert's findings were presented in July 2016 at a roundtable gathering several stakeholders from the public and civil society sectors, organised with the support of the Council of Europe Office in Moldova.

The draft laws are currently enhanced, notably in order to comply with the Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) and the Directive (EU) 2016/680.

2 – Legislative changes and jurisprudence

a) Law No. 87 amending and supplementing certain acts of 28/04/2016

The second element of importance during this period was the adoption on the 28th of April 2016 of the *Law No. 87 amending and supplementing certain acts,* through which a number of amendments related to personal data protection have been included in regulatory acts governing the police and judiciary activity in the Republic of Moldova.

This law amended 8 important legislative acts, namely:

- Criminal Procedural Code
- Contravention Code
- Law on the status of judges

- Law on the National Anticorruption Center
- Law on money laundering and terrorism financing
- Law on police activity and police status
- Law on special investigation activity
- Law on the special investigation officer

These amendments incorporate personal data protection principles in the police and judiciary sectors, including by increasing accountability of the staff from the targeted sectors while processing personal data.

b) Constitutional Court decision No. 16 of 18/05/2016

The Constitutional Court Decision No. 16 of 18 May 2016 on unconstitutionality exception of the Article 10 para. (4) of the Law no. 151 of 30 July 2015 on the Government Agent is relevant to the personal data protection field in the Republic of Moldova.

At the case's origin was the unconstitutionality exception of the Article 10 para. (4) of the Law No. 151 of 30 July 2015 on the Government Agent, issue raised by the representative of the Public Association "Lawyers for Human Rights" within a case that is examined at the Chisinau Buiucani Court, through which the refusal of the Ministry of Justice to provide information on convictions of the Republic of Moldova by the European Court for Human Rights is contested.

The Constitutional Court stated that:

- provisions of the Article 8 of the Law on access to information, according to which personal data are part of official information with limited accessibility and represent data related to an identified or identifiable natural personal whose disclosure would constitute a breach of the right to intimate life, family and privacy, and access to such information is performed in accordance with the provisions of the personal data protection legislation;

- proceeding from the importance of the information related to personal data, the disclosure of which could affect the rights of persons, it benefits from an increased legal protection and have precedence over free access to information in cases expressly provided by law;

- the need to examine, on individual basis, requests related to information held by the Government Agent in a similar manner to the European Court one, without being entirely and automatic exempted the categories of information, as provided by the contested norm from the application of the Law on access to information;

- if a restriction applies only to certain types of information held by the Government Agent, in order not to harm privacy or other legitimate interests, the access to the rest of available information shall be submitted upon request, and if the partial version of a document becomes meaningless or confusing, the access may be denied, according to the Recommendation of the Committee of Ministers of the Council of Europe no. 2 of 21 February 2002 on access to official documents;

- the contested rule does not ensure a fair balance between the right of access to information and protection of rights of other people and, therefore, it is not adapted to a democratic society;

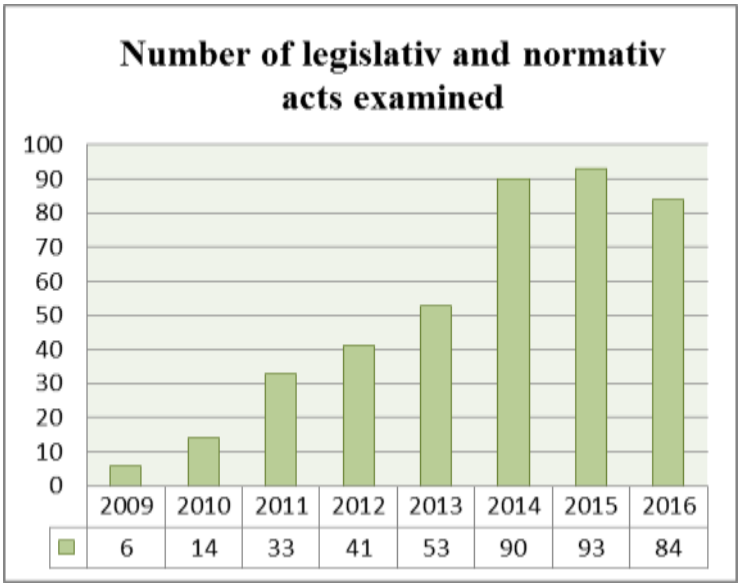
- the provisions of the Article 10 para. (4) of the Law on Government Agent no. 151 of 30 July 2015 transgresses the principle of proportionality, an excessive measure in relation to the objective to

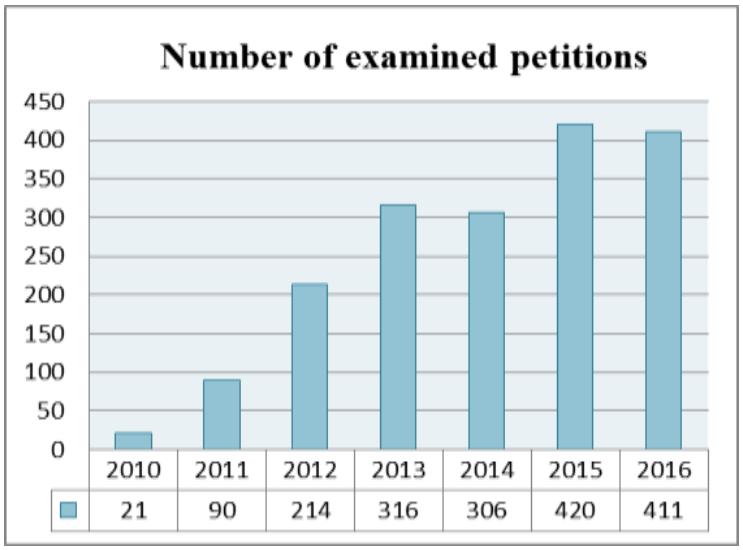
be achieved and thereby contrary to the Article 34 taken together with the Article 54 of the Constitution, -

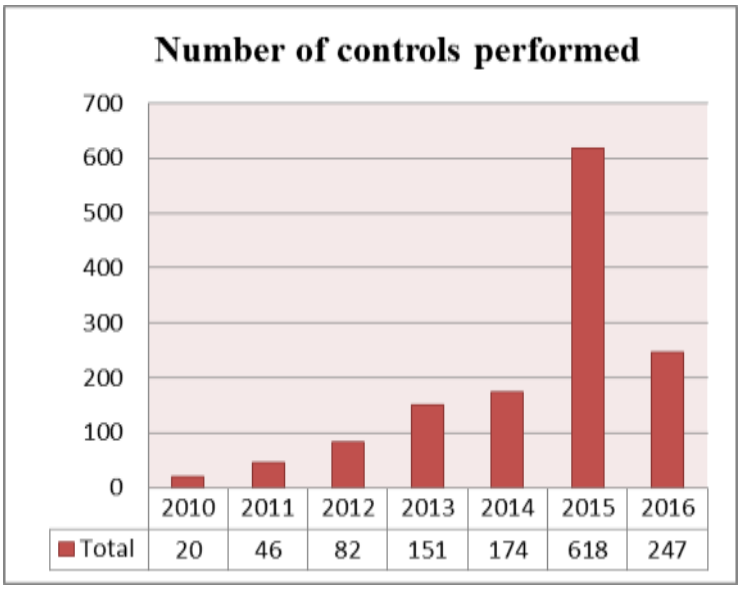
The Constitutional Court admitted the exception of unconstitutionality raised by the representative of the Public Association “Lawyers for Human Rights”, consequently the Article 10 para. (4) of the Law No. 151 of 30 July 2015 on the Government Agent being declared unconstitutional.

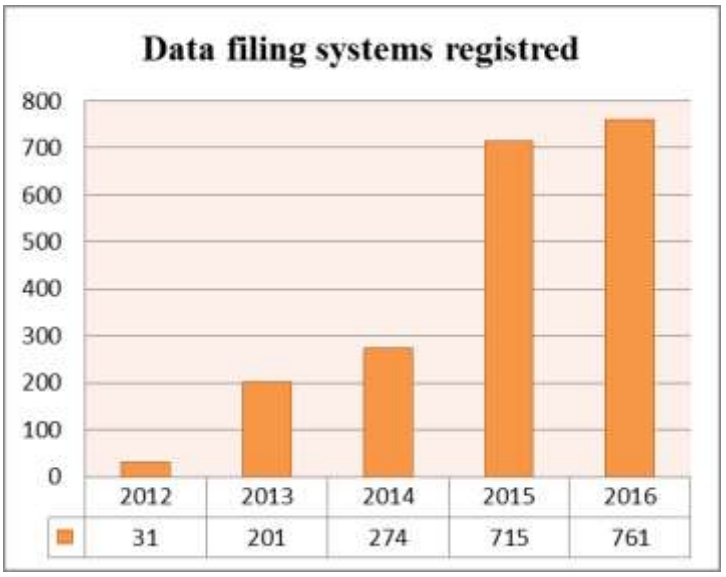
3 – General statistics

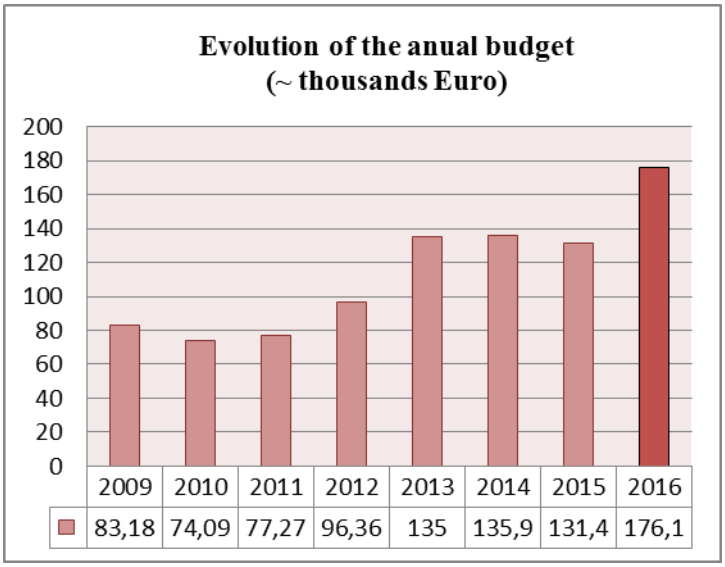
In addition to these major developments, we include several statistics of the NCPDP for 2016 to give additional context in terms of activities and a comparison point with the precedent years.

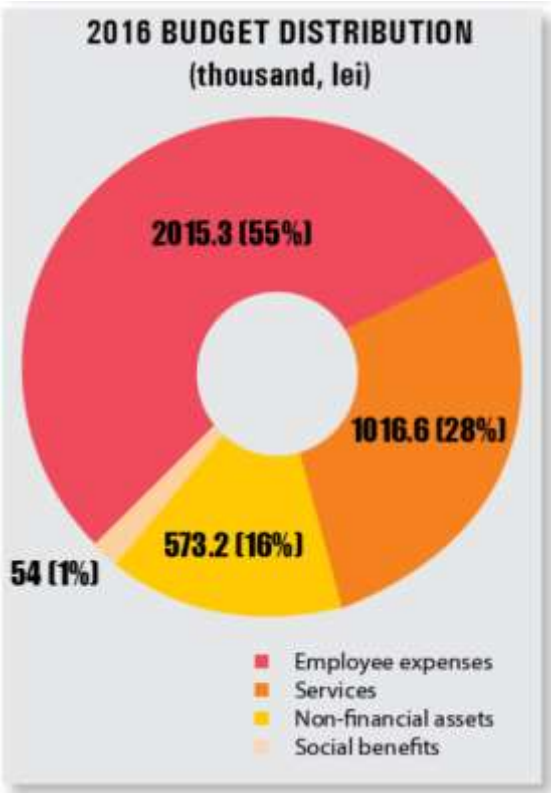









Evolution of the anual budget
(~ thousands Euro)
200
180
160
140
120
100
80
60
40
20
0
2009 2010 2011 2012 2013 2014 2015 2016
83,18 74,09 77,27 96,36 135 135,9 131,4 176,1


2016 BUDGET DISTRIBUTION
(thousand, lei)
2015.3 (55%)
1016.6 (28%)
573.2 (16%)
54 (1%)
Employee expenses
Services
Non-financial assets
Social benefits


INTERNATIONAL COOPERATION
3 cooperation agreements signed
6 working visits
5 participations at conferences

MONACO

PRINCIPAUTE DE MONACO
Développements majeurs intervenus en matière de protection des données personnelles
Période allant de juin 2016 à juin 2017

*****

Lois

Loi n°1.430 du 13 juillet 2016 relative à la préservation de la sécurité nationale;

Loi n°1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique;

Loi n°1.436 du 2 décembre 2016 portant approbation de ratification de la Convention concernant l'assistance administrative mutuelle en matière fiscale ;

Loi n°1.437 du 2 décembre 2016 portant approbation de ratification de l'accord multilatéral entre les autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers ;

Loi n°1.444 du 19 décembre 2016 portant diverses mesures en matière de protection des informations nominatives et de confidentialité dans le cadre de l'échange automatique de renseignements en matière fiscale.

Ordonnance Souveraine

Ordonnance Souveraine n° 6.029 du 9 septembre 2016 modifiant l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la loi n. 1.362 du 03 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Ordonnance Souveraine n° 6.208 du 20 décembre 2016 portant application de la convention concernant l'assistance administrative mutuelle en matière fiscale, de l'Accord multilatéral entre autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers et du Protocole de modification de l'accord entre la Communauté Européenne et la Principauté de Monaco prévoyant des mesures équivalentes à celles que porte la Directive 2003/48/CE.

Arrêtés Ministériels

Arrêté Ministériel n° 2015-68 du 2 février 2015 fixant les bonnes pratiques transfusionnelles;

Arrêté Ministériel n° 2015-69 du 2 février 2015 relatif à la qualification biologique du don du sang (en cours de modification, l'avis de la CCIN a donc été à nouveau sollicité sur le nouveau projet);

Arrêté Ministériel n° 2015-70 du 2 février 2015 relatif à l'hémovigilance et à la sécurité transfusionnelle ;

Arrêté Ministériel n° 2015-71 du 2 février 2015 relatif à la distribution et à la délivrance des produits sanguins labiles;

Arrêté Ministériel n°2016-500 du 5 août 2016 relatif aux modalités de déclaration simplifiée des traitements automatisés d'informations nominatives relatifs à l'organisation des élections des délégués du personnel instituées par la loi n°459 du 19 juillet 1947 portant modification du statut des délégués du personnel, modifiée ;

Arrêté Ministériel n°2016-501 du 5 août 2016 relatif aux modalités de déclaration simplifiée des traitements automatisés d'informations nominatives relatifs à la gestion administrative des salariés ;

Arrêté Ministériel n°2016-502 du 5 août 2016 relatif aux modalités de dispense de déclaration des traitements automatisés d'informations nominatives relatifs à la gestion des fichiers de paie des personnels ;

Arrêté Ministériel n°2016-622 du 17 octobre 2016 portant application de l'article 3 de la loi n°1.430, précitée;

Arrêté Ministériel n°2016-723 du 12 décembre 2016 portant application de l'article 18 de cette même loi ;

Arrêté Ministériel n° 2017-42 du 24 janvier 2017 portant application de l'article 26 de la loi n° 1.435 susmentionnée.

Projets de loi

Dépôt d'un projet de loi relative au consentement et à l'information en matière médicale (déposé au Conseil National).

Recommandations CCIN

Recommandation du 4 janvier 2017 relative aux traitements automatisés d'informations nominatives ayant pour finalité *« La gestion des obligations légales relatives aux échanges automatiques d'informations à des fins fiscales »* ;

Recommandation du 19 avril 2017 sur les dispositifs d'enregistrement des conversations téléphoniques mis en œuvre par les établissements bancaires et assimilés (laquelle annule et remplace la recommandation précédente en date du 16 juillet 2012) ;

Recommandation du 19 avril 2017 relative aux traitements automatisés d'informations nominatives ayant pour finalité *« La gestion du contentieux* ».

NORWAY / NORVEGE

Major developments in the Norwegian legislation on protection of personal data

To: The Secretariat

From: The Norwegian Ministry of Justice and Public Security

Date: 01.06.2017

1. INTRODUCTION

We refer to the Secretariat's email 27 April 2017. Below is an update on the major legal developments in Norway concerning personal data protection since the 33th meeting of the T-PD.

2. DATA PROTECTION LEGISLATION

Norway has worked on preparing the necessary draft proposals for legislative amendments for the implementation of Regulation (EU) 2016/679 (General Data Protection Regulation). The General Data Protection Regulation, when implemented in the EEA-agreement, will require a complete revision of the Norwegian Data Protection Act, in addition to a number of amendments of data protection provisions in sector-specific legislation.

A proposal for amendments to the act on the processing of personal data in the police sector, implementing Directive (EU) 2016/780 on data protection in the police and criminal justice sector, was submitted to the Norwegian Parliament in April 2017.

3. ACTIVITIES OF THE SUPERVISORY AUTHORITY

In 2016, The Norwegian Data Protection Authority focused its activities in particular on the justice sector, the digitalization of the public sector, the health and welfare sector and the commercial use of consumers' personal data. The Data Protection Authority registered 1745 new cases in 2016, and received 206 notifications on personal data breaches that caused unauthorised disclosure of personal data. Both figures are higher than in previous years.

POLAND / POLOGNE

Country report on major developments in the data protection field

I. Legislation

1. Recent National Developments – legal framework

On 7 October 2016 the Act on trust services and electronic identification entered into force. The Act repeals the existing legal provisions in this regard on electronic signature and introduces the provisions of the eIDAS Regulation to be applied. In particular, the Act modifies 82 acts as regards the issues of identification and electronic signature, including the Code of Administrative Proceedings, the Act on providing services by electronic means and the Act on informatisation of entities performing public tasks.

On 2 July 2016 the Anti-terrorism Act entered into force, which – despite of GIODO's objection – introduced registration of prepaid cards and grounds for collection of materials from operational activities without regulation of the storage period. The principles of exercising supervision over activities carried out in relation to suspected persons also raised GIODO's doubts. The Act sets forth that decision on monitoring suspected persons and carrying out operational activities shall be taken by the Public Prosecutor General without notifying the court. Moreover, the Act provides for keeping a list of persons who may be related to terrorism, without specifying the scope of information contained on the list as well as its storage period, which was requested by GIODO. GIODO raised also objections concerning the right to block access to ICT services, requesting their further specification and the possibility to appeal from the decision in this regard to the court. The comments presented by GIODO were not taken into account.

On 21 October 2016 the Sejm of the Republic of Poland (lower chamber of the Polish Parliament) adopted the Act on the national tax administration, which modifies tax administration organisation. In GIODO's view the Act entitles tax authorities to non-defined scope of personal data processing. The Act does not indicate the scope nor the period of storage of the data collected from tax payers. At the stage of legislative works, GIODO drew attention to incompliance of proposed provisions with the currently binding Act on Personal Data Protection and with the General Data Protection Regulation by the Parliament and by the Council. Those opinions were not considered.

II. Ahead of the EU data protection reform

On 27 June 2016 GIODO appointed the Experts Commission for the reform of personal data protection in the EU, including next to GIODO's experts also experts from various milieus, e.g. DPOs. Its task is to analyse essential legislative changes in the Polish legal system in connection with the entry into force of the GDPR. The Commission will also draw up opinions and studies on specific solutions adopted in the GDPR.

On 8 July 2016 the Polish DPA appointed from among its employees the Team for Personal Data Protection Reform in the EU.

Within the framework of preparations for the implementation of the new EU data protection framework, GIODO has been undertaking a variety of educational activities for the purpose of increasing awareness of both data subjects and Data Protection Officers, including for example conferences, trainings, workshops etc. (see point III Events below). Also, the experts from the Polish DPA developed a Guide for DPOs "Performance of DPOs Duties in the Light of the General Data Protection Regulation". Moreover, GIODO drew up a set of questions which are to help the data controllers to evaluate the state of their preparation for the application of the new law.

III. Events

On 7 December 2016 in Warsaw a Poland-wide Conference entitled “Implementation of the General Data Protection Regulation – Procedural Aspects” was organised by GIODO, the President of the Supreme Administrative Court and the Dean of the Faculty of Law and Administration of the University of Warsaw. The event was attended by over 200 persons representing administrative courts, public administration, as well as academics and entrepreneurs. The conference focused on selected topical issues which required discussion before commencing the application of the GDPR.

Moreover, in 2016 GIODO launched a series of trainings for Data Protection Officers (DPOs) from selected sectors. In 2016 the Polish DPA carried out 2 trainings for DPOs from the public sector (28 June and 9 September 2016) and the higher education sector (24 November 2016). In 2017 GIODO conducted 2 trainings for DPOs from the medical sector (1 and 2 March 2017) and a training for DPOs from the Polish courts (23 May 2017).

In 2017, just like in previous years, GIODO celebrated, already for the 11th time, the European Data Protection Day. As each year, conferences devoted to most recent issues related to the right to privacy and data protection are held, including:

31 January 2017, Warsaw – the Conference on Personal Data Protection in the Era of Changes organised by GIODO. The possibility to obtain legal advice on personal data protection provided by GIODO’s representatives.

3 February 2017, Dąbrowa Górnicza – Open Day of the Inspector General for Personal Data Protection organised by the University of Dąbrowa Górnicza at its premises in cooperation with GIODO.

Furthermore, in January/February 2017 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.

On 23 March 2017 in Krakow GIODO organised the subsequent Meeting of DPAs from the Visegrad Group Countries, focused mainly on discussing and exchanging experiences related to the application of the General Data Protection Regulation, having in mind proper preparation of DPAs for new challenges.

IV. GIODO projects and programmes

Within its educational activity, GIODO is inter alia involved in realising EU co-funded projects. In the reporting period the Polish DPA continued implementation of the project co-funded by the Fundamental Rights and Citizenship Programme of the EU - 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.

The subsequent PHAEDRA II Project Workshop was organised by GIODO on 18 October 2016 in Marrakech, within the framework of the 38th International Conference of Data Protection and Privacy Commissioners. It was devoted to cooperation of European Data Protection Authorities from the perspective of „trust".

Moreover, GIODO is one of the partners of a project funded by the European Commission Erasmus+ "Key Action - Cooperation for Innovation and the Exchange of Good Practices, Action - Strategic Partnerships for Higher Education". The realised project is aimed at developing an innovative programme of postgraduate studies regarding personal data protection, which would meet market needs. The coordinator of the project is the University for Information Science and Technology St. Paul the Apostle, Ohrid (Macedonia) and the partners of the project are the Inspector General for Personal Data Protection (Poland), the Directorate for Personal Data Protection (Macedonia), the Commission for Personal Data Protection (Bulgaria) and the University of Lodz (Poland). The project shall be realised within 28 months.

V. Agreements on cooperation

In the reporting period GIODO concluded agreements on cooperation on the protection of privacy and personal data with a dozen or so institutions, including inter alia the banking, insurance and Internet sector, universities, the Supreme Administrative Court, the Ombudsman for Children and the Polish Chamber of Information Technology and Telecommunications.

SERBIA / SERBIE

Inadequate legal framework remains the main issue in the field of personal data protection. Enactment of the new Law on Personal Data Protection has been delayed on several occasions. The Law should have been enacted by the end of 2016. A new time limit for enactment of the Law has not been defined.

In order to facilitate the improvement of the state of play in this area, the Commissioner for Information of Public Importance and Personal Data Protection and his team have prepared the Model Law on Personal Data Protection, in accordance with the General Data Protection Regulation. Public consultations on the Model are underway. After the public consultations, the plan is to submit the agreed text of the Model to the Government and the Ministry of Justice for consideration.

SLOVENIA / SLOVENIE

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD (2016)

Report by the Information Commissioner of the Republic of Slovenia

A. Summary of activities

The Information Commissioner of the Republic of Slovenia is the inspection and offence authority in the area of data protection as provided by the Personal Data Protection Act of Slovenia (PDPA).

In 2016 the Information Commissioner (IC) initiated 683 inspection cases, 245 in the public and 438 in the private sector. The IC also initiated 83 offence procedures. The offences mainly concerned unlawful video surveillance, direct marketing and disclosure of data to unauthorized users. Inadequate data security and traceability of data processing have also been identified as a problematic area. In 2016 the IC increased the number of planned ex officio supervisions in sectors such as the police, health institutions, banks, insurance companies, public administration bodies, schools and faculties and the energy sector.

In addition to the inspection and offence authority competences 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 2016 the IC issued 1330 written opinions and clarifications and gave more than 2500 clarifications over the phone. In 2016 more than a 100 data controllers have requested prior consultation with IC regarding legislation, solutions or projects in development. The IC is under PDPA also competent to conduct prior checks regarding biometric measures (4 cases), transfer of data to third countries (53 cases) and connection of filing systems (4 cases). The data controllers in such cases need to obtain the IC's permission in a form of administrative decision. The IC is also the appellate authority regarding access to an individual's personal data (91 cases). The IC issued 120 opinions on legislative proposals.

B. Information on interesting case-law

1. Inadequate data security by healthcare institutions

IC has conducted a number of ex officio supervisions in the healthcare sector, the public and private sector providers and found that in this sector there are still a number of pressing issues, mostly pertaining to inadequate data security, such as:

- Transmission of health related data using unencrypted communications
- Inappropriate use of authentication means (e.g. persons sharing accounts, etc.)
- Limited transparency of contractual data processing
- Lack of awareness about appropriate policies regarding disclosure of patient's data
- Inappropriate physical security of spaces where patient's documentation is kept.

IC will hence continue its activities of increased supervision in this sector.

Additionally, IC received a complaint about a health service website were unlimited access to sensitive patients' and employees' data was possible by entering a specific URL into the browser. IC found that the service did not request any additional verification or authorization of users who should be granted access to the website service. The data controller was notified about the security incident and ordered immediate corrective actions to adequately protect the patients' and employees data contained at the website. The data controller implemented corrective measures and notified the national CERT about the security incident. It also provided clarification and proof that the data was only accessed by the researcher who discovered the security vulnerability.

2. Identification of individuals, alleged of not paying parking tickets in Croatia, based on licence plates numbers

Information Commissioner initiated an inspection procedure against a law firm, based in Slovenia that was acquiring personal data of Slovenian citizens that have allegedly not paid parking tickets in Croatia and Serbia and have been served payment notices by a foreign company specialized in fee collection. Personal data of Slovenian citizens were acquired by a Slovenian law firm, based on the registration plate numbers, from different administrative unites in Slovenia, that have access to the record of registered vehicles. The collected data were sent to the foreign company in bulk – namely the data on all citizens who have allegedly not paid the parking tickets, and not only the data of those who have actually not paid their dues upon receipt of the payment notice. Upon identification of the registration plate number holders, the foreign company sent individuals a reminder before enforcement, requesting them to pay the allegedly outstanding parking ticket fee and, additionally, the costs of the reminder.

Information Commissioner found that the law firm only had legal basis for identification of those individuals that have not paid the outstanding debt after being notified by the foreign company. Since the law firm collected the data on app. 1500 individuals and could only show outstanding debt for 500 individuals, the IC held that the law firm needed to delete the data acquired on all other individuals where it was not clear that their debt still exists and the data will be necessary in a court procedure.

3. Inadequate security of telecommunications data

IC received a complaint concerning a security vulnerability of a telecommunications provider. A database of its e-mail servers, containing the senders and recipients e-mails, IP addresses and time stamps was found to be accessible online to unauthorised persons, using a "Telnet" protocol. The vulnerability was a consequence of a non-working firewall and lack of other security measures the provider should have implemented, such as periodic checks of security settings, traceability measures, etc. IC found that the telecommunications provider did not implement appropriate data security measures provided by PDPA as well as possibly by the Electronic Communication Act, supervised by the national telecommunications regulator, Agency for Communication Networks and Services. Both supervisory authorities established close expert cooperation in this case.

C. Other important information

In the course of its awareness raising activities the IC continued its preventive work (lectures, conferences, workshops for different public groups), altogether the experts conducted more than 100 lectures. Together with the Centre for Safer Internet of Slovenia it covered awareness rising activities for children and youngsters. The Information Commissioner also published several new guidelines on various data protection topics: Guidelines on BYOD, Guidelines on Central Registry data protection issues, Guidelines for multitenant building managers, Guidelines on data protection in employment relationships.

In the context of the European Data Protection Day 2016 the IC hosted a panel discussion “Will the rights of individuals and obligations of data controllers change with the new Data Protection Legislation”. The focus was on the improvements brought by the GDPR in terms of rights of individuals and the challenges for different stakeholders on the way to compliance. At the event, as per tradition, the awards for good practice in data protection were presented to selected data controllers.

In terms of policy issues the IC has dealt with extensively, the new General Data protection Regulation and the accompanying Directive concerning law enforcement sector is the first to be mentioned. IC has been analysing the provisions in depth and actively contributing to the work of Article 29 Working Party in this regard, as well as contributing to the national discussions regarding implementation of the new EU data protection framework. In this regard it is necessary to mention the increasing development in the fields of smart phones that are becoming the main point of identification of users who access different systems with phones – banking, communications, internet, access to electric cars, hotel rooms, boarding passes, etc. Profiling and development of artificial intelligence are another field where individuals are facing grave consequences if they are subject to decisions based on algorithms and their rights are not respected. Issues regarding genetic and biometric data, together with ever more devices connected to the internet of things, are the reality data protection authorities will be facing in the coming years.

The IC also participated in a number of international events and bodies such as: The Article 29 Working Party, Joint Supervisory Body of Europol, Joint Supervisory Authority for Schengen, Joint Supervisory Authority for customs, EURODAC, WPPJ, International Working Group on Data Protection in Telecommunications, Council of Europe’s Consultative Committee under the Convention 108 (T-PD).

In a consortium with partners from different EU Member States the IC was involved in a 3 year EU FP7 project CRISP, which focuses on evaluation and certification schemes for security products. The IC was 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.

SWITZERLAND / SUISSE

Développements majeurs intervenus dans le domaine de la protection des données

Suisse

Le 21 décembre 2016, le Conseil fédéral a mis en consultation l'avant-projet de révision de la loi fédérale sur la protection des données. L'objectif de cette révision est d'adapter notre législation aux technologies et à la société actuelle, de renforcer la protection des données et de renforcer la compétitivité de la Suisse et son attractivité pour le numérique. Elle doit permettre de ratifier la Convention 108 modernisée, de transposer la directive de l'Union européenne relative à la protection des données personnelles traitées à des fins de poursuite pénale et d'entraide en matière pénale, de se rapprocher du niveau de protection des données du règlement européen et de maintenir la reconnaissance d'un niveau de protection des données adéquat.

La révision doit renforcer le droit à la protection des données afin que tout un chacun puisse retrouver une plus grande maîtrise sur les informations qui le concernent. Cela passe par une plus grande transparence des traitements et l'octroi de nouveaux droits tel que le droit de ne pas être soumis à une décision automatisée sans pouvoir faire valoir son point de vue ou le droit de connaître la manière dont de telles décisions sont prises. La révision vise également à renforcer et concrétiser les obligations des responsables de traitement. Elle prévoit d'introduire notamment une obligation d'annonce des violations de la protection des données, l'obligation de procéder à des études d'impact de protection des données et une obligation de documenter les traitements. Elle introduit également les principes de la protection des données dès la conception et de la protection des données par défaut. La révision doit également renforcer les compétences du PFPDT qui se verra conférer un pouvoir de décision. Le préposé devrait également à l'avenir pouvoir émettre des recommandations de bonnes pratiques élaborées en coopération avec les milieux intéressés ; ainsi qu'approuver ou reconnaître des règles contraignantes d'entreprises dans le cadre des transferts de données à l'étranger. De même, il devrait édicter, reconnaître ou approuver des clauses contractuelles standards. Le Conseil fédéral devrait à l'avenir prendre des décisions sur le niveau de protection adéquat d'un Etat tiers. Les possibilités de coopération avec d'autres autorités de protection des données en Suisse et à l'étranger et d'entraide administrative sont également améliorées. La révision devrait aussi permettre aussi un renforcement significatif des sanctions.

En outre, la transposition de la directive relative à la protection des données personnelles traitées à des fins de poursuite pénale et d'entraide en matière pénale entraîne la modification de plusieurs lois sectorielles dans le domaine de la police et de la poursuite pénale.

Le Conseil devrait transmettre à l'automne le projet de loi au Parlement fédéral.

TUNISIA / TUNISIE

INPDP

الهيئة الوطنية لحماية المعطيات الشخصية

INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES

NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

La Tunisie est précurseur dans son environnement arabe et africain dans le domaine de la protection des données personnelles. C'était le seul Etat dans cet espace qui a constitutionnalisé la protection en 2002 et qui édicta une loi organique de protection en 2004 (105 articles). L'Instance de protection a été mise en place en 2008.

Le constituant de 2014 confirmera la place de cette protection dans le corpus juridique en l'élargissant. L'article 24 stipule que « L'État protège la vie privée, l'inviolabilité du domicile et le secret des correspondances, des communications et des données personnelles » réaffirmant ainsi la volonté politique d'élargir la protection.

Le Chef du Gouvernement édicta le 12 octobre 2016 une circulaire à l'intention de toutes les personnes publiques réaffirmant l'impérieuse nécessité de respecter les normes dans ce domaine et de coordonner les actions tendant à l'amélioration de la protection avec l'Instance (INPDP).

Depuis la mise en place de la nouvelle formation de l'Instance, en décembre 2015, des actions prioritaires furent planifiés :

- Développer une **culture de la protection** au sein de la société tunisienne
- **Solliciter les responsables de traitement** des données personnelles pour respecter les normes découlant dans la loi de 2004
- Transmettre les dossiers des responsables récalcitrants au **Procureur de la République** pour appliquer les sanctions pénales prévues par la loi
- **Rehausser du niveau de protection** des données personnelles en se conformant aux normes internationales et en mettant à jour le cadre juridique national

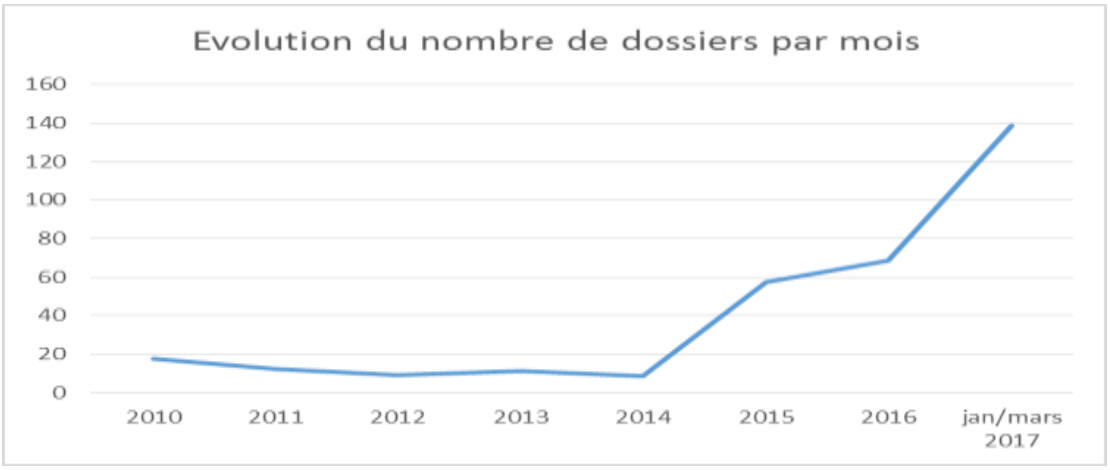
Depuis le début de l'année 2016, l'Instance a entrepris les **actions suivantes sur le plan national** :

- Effectuer un **sondage d'opinion** pour évaluer le niveau de culture des tunisiens et tunisiennes dans le domaine de la protection des données personnelles. Les résultats rendus publics à l'occasion d'une conférence de presse démontrent la quasi absence de connaissance des citoyens dans ce domaine ce qui explique leur manque de réaction concernant les violations des règles de protection.
- Développer une **présence médiatique** de l'Instance aussi bien sur le plan radiophonique que télévisuels. Ces apparitions installent la protection des données dans le vécu tunisien et suscitent des réactions aussi bien de la part des responsables de traitement que des citoyens. Des interviews dans les plus grands organes de presse écrite ont permis aussi de susciter une réflexion parmi les décideurs et les citoyens autour de cette question. C'est devenu un sujet important dans le cadre de la transition démocratique que connait a Tunisie depuis 2011.
- L'instance a suscité le lancement des premiers travaux de **recherche sur le plan universitaire et à l'Ecole nationale d'administration** portant sur la problématique de la protection des données personnelles. Dans ce cadre, elle a été invitée à intervenir dans les enseignements à la faculté de médecine ou les institutions d'informatique ...
- Les intervenants sur le plan économique n'ont jamais été confrontées à cette problématique et ne connaissent pas les obligations qui leur incombent dans ce domaine. L'Instance entama ainsi une action de **sollicitation des responsables de traitement des données personnelles**. Une campagne prit deux formes : La première permit d'envoyer de manière nominative des lettres de rappel des obligations aux acteurs dans certains domaines qui paraissent très demandeur de traitement de données personnelles. Cette action toucha les partis politiques, les entreprises publiques et établissements publics, les centres d'appels, les hôtels, les cliniques, les hôpitaux, les centres de dialyse, les laboratoires médicaux et les institutions de radiologie … Quelques 1300 lettres ont été envoyées. La deuxième entreprit de toucher les structures représentants certains domaines ou chargé de les contrôler ou réguler. Prioritairement elle toucha le comité national d'éthique médicale, les comités de protection des personnes, l'ordre des médecins et des pharmaciens, le comité général des assurances, l'association des professionnels des banques, les chambres syndicales appartenant à l'union patronale, l'Instance nationale des

télécommunications, l'agence nationale de sécurité informatique, l'instance nationale de certification en matière de santé, l'Institut national de la consommation …

- Grace à sa politique proactive depuis 2015, l'Instance a vu se **développer la masse des dossiers** qui lui sont soumis.

- La moyenne des dossiers traités par mois a subis une évolution exponentielle mettant à rude épreuve les capacités de traitement de l'Instance et suscita une demande de dotation en personnel supplémentaire.



- L'Instance organisera ou prendre part à des **conférences autour de la protection des données personnelles**. Ces interventions touchèrent principalement le monde des technologies, de la communication, de la santé ainsi que la protection des consommateurs. En une année plus de 50 conférences dans tous les domaines ont été présentées sur tout le territoire national.
- La **société civile tunisienne** a commencé à s'intéresser à la problématique de la protection des données personnelles. L'association leaders du suivi de la transition démocratique en Tunisie depuis 2011, Bawsala (La boussole) a proposé de réaliser un **livre blanc** sur la protection des données en Tunisie. Ces axes tourneront autour du constat de la situation de la protection, le benchmarking international, les propositions et recommandations pour les années à venir dans ce domaine.
- L'INPDP a été impliqué dans plusieurs **commissions de travail sur des projets nationaux** : la carte d'identité biométrique, la classification des données publiques, Mais aussi l'INPDP est

représenté dans la composition d'autres instances : Agence technique des télécommunications, Instance nationale d'accès aux données. Enfin elle a été chargée de concevoir le cadre juridique et de contrôler la mise en place du projet d'identifiant unique citoyen par le ministère des collectivités locales.

- Mise en place en collaboration avec **l'Agence nationale de la sécurité informatique** d'un référentiel technique de protection des données personnelles à l'intention des auditeurs de sécurité informatique. Ce référentiel permettra aux auditeurs à l'occasion de l'audit obligatoire de sécurité informatique de vérifier si le responsable de traitement a pris les mesures techniques nécessaires pour préserver la sécurité de ces données personnelles.
- L'Instance a suscité l'édiction d'un **texte national sur la cybercriminalité** qui permettra d'adhérer à la convention de Budapest. Le projet est actuellement en étape de finalisation avec le conseiller à la législation du Chef du Gouvernement. Il devrait être approuvé en conseil de ministre et passer au Parlement avant la fin du mois de mai 2017.
- Rédaction d'un **nouveau projet de loi sur la protection des données personnelles qui remplacera la loi de 2004** dépassée sur plusieurs aspects. La nouvelle loi permettra de prendre en considération les nouvelles normes incluses dans le règlement européen 2016/679. Le projet comprend plus de 230 articles et entame en mai 2017 la procédure de consultation des entités publiques et privées ainsi que de la société civile. Des workshops seront organisés pour en débattre et le projet devrait être soumis à l'adoption du Conseil des ministres au début du mois de septembre 2017. L'adoption de la loi par le Parlement est prévue pour le premier trimestre 2018.
- Développement en cours d'un **nouveau site web** de la protection qui permettra entre autre de réaliser toutes procédures légales en ligne ainsi que le dépôt de plaintes de la part des citoyens.
- Développement en cours d'une **application de téléphonie** permettant d'expliquer les droits des citoyens en matière de protection des données personnelles et permettra de porter plainte en ligne.
- L'Instance a décidé la transmission les **dossiers des responsables récalcitrants au Procureur de la République**. A partir de juin 2016 des dizaines de requêtes sont entre les mains de la garde nationale pour leur instruction. L'Instance a demandé l'application de l'article 90 de la loi de 2004 qui punit le non-respect des obligations par les responsables de traitement d'une amende et d'une sanction privative de liberté. Il est à signaler que ce sont là les premières actions en justice entreprises par l'Instance depuis sa création. D'un autre côté, une décision de l'Instance a fait l'objet en septembre 2016 d'une action en justice et c'est aussi la première fois qu'un acte de l'Instance est porté en appel devant la justice.
- Ediction en 2016 d'une **délibération déterminant les Etats considérés comme ayant une protection adéquate** et vers lesquels le transfert de données personnelles ne devrait pas poser de problèmes conformément à l'article 51 de la loi tunisienne.
- Ediction à l'intention des partis politiques d'une **délibération encadrant le traitement des données personnelles dans leur activité politique et pendant les périodes électorales**. La délibération sera édictée par l'instance nationale de protection des données personnelles avec l'Instance supérieure indépendante des élections. Cette délibération s'impose puisque la Tunisie organise les élections communales en décembre 2017.

Depuis le début de l'année 2016, l'Instance a entrepris les **actions suivantes sur le plan international** :

- **Adhésion à la convention 108 du Conseil de l'Europe** : En juillet 2015, la Tunisie a introduit sa demande d'adhésion à la convention 108 et son protocole 181 du Conseil de l'Europe. Ce dernier l'invita officiellement à y adhérer le 2 décembre 2015. Depuis le processus interne a permis d'entamer le processus de ratification par une loi nationale. Le projet a été transmis par le gouvernement au Parlement le 9 mars. La commission des droits et des libertés a auditionné le Président de l'INPDP à ce sujet le 14 avril. Le projet sera soumis au vote de la plénière avant la fin de mai 2017. Il est à signaler à cet égard que la constitution tunisienne de 2014 donne aux conventions dûment ratifiées une valeur supra législative.

- **Co-organisation avec Monsieur le rapporteur spécial des Nations Unies chargé de la protection de la vie privée un workshop régional** sur la « Vie privée, la personnalité et le flux des données » qui se tiendra les 25 et 26 mai 2017 à Tunis. Plus de 330 experts et compétences internationales y prendrons part ainsi que plus de 40 intervenants tunisiens.
- **L'Association francophone des protecteurs de données** (AFAPDP) dont l'INPDP assure la vice-présidence depuis 2016 a décidé la tenue en Tunisie du 6 au 9 septembre 2017 des manifestations suivantes :
    - La conférence nationale de l'AFAPDP qui portera probablement sur les implications de l'entrée en vigueur du nouveau règlement européen. L'association en profitera pour célébrer son dixième anniversaire.
    - L'assemblée générale de l'association
    - Deux journées de formation au profit des agents des autorités de protection membres de l'association.
- Abriter la **réunion annuelle du réseau africain** de la protection des données personnelles en septembre 2017. La Tunisie a accueilli favorablement la tenue de cette manifestation avant celle de l'AFAPDP.

ASSOCIATION EUROPEENNE POUR LA DEFENSE DES DROITS DE L'HOMME / EUROPEAN ASSOCIATION FOR THE DEFENSE OF HUMAN RIGHTS (AEDH)

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

Bulgarie

Législation : La Bulgarie n'a pas modifié son cadre législatif en matière de protection des données personnelles. Pour autant, le « E-Governement Act » de juillet 2016 a eu un impact indirect sur celle-ci. Aucune réforme de la protection des données n'est à ce jour entamée.

Rapports annuels : Depuis 2006, un rapport est effectué chaque année sur l'état de la protection des données en Bulgarie par l'autorité de contrôle.

Droit d'accès : Les personnes concernées ont accès et peuvent rectifier les données les concernant par l'intermédiaire de l'autorité de contrôle.

Jurisprudence : La Cour constitutionnelle a jugé inconstitutionnelle la loi de 2016 qui exigeait que les e-cartes contenant les informations des individus en matière de santé contiennent l'identité biométrique des citoyens bulgares.

Défis : Les prochains défis à relever pour la Bulgarie en matière de protection des données seront multiples. D'abord, le pays va devoir se préparer à l'introduction du nouveau cadre juridique de la réforme européenne en matière de protection des données. Il devra poursuivre la préparation de la présidence bulgare en 2018 concernant la « Protection des données personnelles ».
Enfin, la Bulgarie devra poursuivre les efforts dans le domaine de la protection des données personnelles pour l'adhésion à Schengen et maintenir l'acquis de Schengen dans la situation internationale compliquée.

France

Législation

Etat d'urgence

La France vit toujours sous le régime de l'Etat d'urgence depuis novembre 2015, elle avait alors alerté le Secrétaire général du Conseil de l'Europe des risques de dérogation à la Convention européenne des droits de l'homme. Cette atteinte aux droits et aux libertés n'assure pas pour autant la sécurité promise.
Alors que l'état d'urgence a été prorogé jusqu'au 14 juillet 2017, un projet de loi du 8 juin 2107 prévoit d'intégrer dans le droit commun la plupart des mesures de l'état d'urgence y compris la saisie de données informatiques lors des perquisitions administratives (l'autorité administrative devant demander au juge des référés du tribunal administratif l'autorisation d'exploiter ces données personnelles.) http://www.ldh-france.org/lettre-ouverte-au-premier-ministre-transparence-donnees-en-lien-mise-en-oeuvre-letat-durgence/

Création du fichier TES

Octobre 2016 publication du décret TES (« Titres électroniques sécurisés ») portant création d'un fichier centralisant les données d'identité, de filiation et de biométrie de l'ensemble des Français. En l'absence de tout contrôle parlementaire puisque l'article 27 de la loi « informatique et libertés » du 6 janvier 1978 laisse au gouvernement la faculté d'instituer, par un simple décret, tous traitements de données à caractère personnel pour le compte de l'État, ou touchant à la sécurité nationale, les données biométriques étant soumises au même régime. Le fichier TES rassemble l'ensemble des informations d'état civil, de filiation, la photo d'identité, le domicile, éventuellement le courriel, mais également la couleur des yeux ou les empreintes digitales. La finalité du fichier TES : rationaliser la délivrance des titres d'identité (et supprimer des postes de fonctionnaires) ne justifie pas le choix de la centralisation du fichier qui est un choix dangereux en termes de sécurité et de garanties d'intégrité : il expose un ensemble massif et précieux de données personnelles à la portée de puissances hostiles ou de criminels expérimentés. (http://www.ldh-france.org/fichier-tes-danger-les-libertes/)

Publication de la « loi pour une république numérique »

Octobre 2016, la loi reconnait aux personnes concernées un droit à « l'autodétermination informationnelle » y compris la possibilité de prévoir le sort de ses données après sa mort. Elle renforce certains pouvoirs de l'Autorité de protection des données (la CNIL) comme des pouvoirs de sanction renforcés et lui donne de nouvelles missions comme la conduite d'une réflexion sur les problèmes éthiques soulevés par l'évolution des technologies numériques.

Rapports annuels

La CNIL a publié son 37e rapport annuel. Elle recense notamment 7700 plaintes dont 410 suite à des refus de demandes de déréférencement auprès des moteurs de recherche.
https://www.cnil.fr/fr/mediatheque/rapports-annuels

Défis

Mise en œuvre du RGPD : La commission des lois de l'Assemblée nationale a mis en place une Mission d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française qui a procédé à de nombreuses auditions dont l'AEDH le 1er février 2017.
http://www.assemblee-nationale.fr/14/rap-info/i4544.asp

La CNIL a lancé des consultations ouvertes au grand public sur différents points du RGPD.
https://www.cnil.fr/fr/reglement-europeen-consultation-sur-le-profilage-consentement-notification-de-violations

Grèce

Législation : La Grèce n'a pas modifié son cadre législatif en matière de protection des données depuis la Loi 3917/2011 portant sur la conservation des données. Pour autant, deux processus de modification sont en cours.

Ainsi, une commission parlementaire a été mise en place afin de travailler avec le ministère de la Justice sur la réforme de la protection des données lancées par la Commission européenne afin de transposer la directive 2016/680 et d'inclure certaines dispositions non-inclues dans le Règlement général sur la protection des données.

Une commission parlementaire travaille également étroitement avec le Ministère de l'Intérieur pour la transposition de la Directive 2016/681 sur le PNR Européen.

Rapports annuels : L'article 19 de la Loi 2472/1997 sur la protection des données personnelles prévoit que l'Autorité de Protection des Données Personnelles soumette un rapport annuel au Parlement. Pour autant, les rapports ne sont pas publiés régulièrement.

Droit d'accès : Concernant le droit d'accès et de rectification, il est prévu aux articles 12 et 13 de la Loi 2472/1997. La personne concernée accède directement à ses données auprès du responsable du traitement et si elle n'est pas satisfaite, elle a le droit de déposer une plainte auprès de l'Autorité de contrôle.

Jurisprudence : Un arrêt significatif (arrêt 1/2017) a été rendu par la Cour de Cassation grecque : elle a validé un traitement des communications électroniques d'un ex-directeur qui donnait des informations à une entreprise compétitive.

Défis : Les prochains défis à relever en matière de protection des données personnelles sont divers. En premier lieu, il y a la transposition de la directive PNR pour laquelle une commission parlementaire a été créée auprès du Ministère de l'Intérieur afin de mettre en place ce système.
En termes de données personnelles, une base de données est en train d'être créée pour le ministère de la Santé pour une gestion plus aisée du système national de santé.
Enfin, la Grèce doit également se préparer à la mise en œuvre du RGPD.

Hongrie

Législation : La Hongrie a amendé sa constitution : elle permet désormais au gouvernement de statuer par décret, en cas de menace terroriste, de lancer des mesures de surveillance accrue notamment de l'Internet.

Rapports annuels : L'autorité de protection des données (APD) nationale publie un rapport annuel.

Droit d'accès : Les personnes concernées ont accès à leurs données directement auprès des responsables des fichiers. Elles ont droit à une demande gratuite par année ensuite elles doivent payer des charges pour les demandes suivantes.

Défis : Les prochains défis à relever pour la Hongrie en matière de protection des données personnelles est la direction d'un projet pilote PNR (« Programme pilote d'échange de données des unités d'information des passagers ») ainsi que la mise en œuvre du RGPD.

Lettonie

Législation : La Lettonie a voté la mise en œuvre du système PNR. En mai 2017, le Cabinet a adopté sa position pour la proposition de la Commission concernant le RGPD.

Rapports annuels : Des rapports annuels sont publiés régulièrement.

Droits d'accès : Les personnes concernées ont un droit d'accès directement auprès du responsable du traitement et peuvent faire appel auprès de l'autorité de contrôle en cas d'absence de réponse.

Défis : Les défis auxquels va être confrontée la Lettonie est la mise en place d'un système PNR ainsi que la mise en œuvre du RGPD.

Pologne

Législation : La Pologne a modifié sa législation en matière de protection des données personnelles. Ainsi, la loi du 10 Juin 2016 prévoit la collecte d'informations au nom de la menace terroriste potentielle ainsi que pour les étrangers sur lesquels pèsent des suspicions, notamment sur la légalité de leur entrée. La loi prévoit un accès pour l'Agence de sécurité intérieure à de très nombreuses bases de données.

Rapports annuels : Sur le site de l'Autorité de protection des données, les rapports annuels datent de 2003 et 2004 pour la version anglaise.

Droit d'accès : Les personnes concernées peuvent obtenir les informations auprès du responsable du traitement. Ce droit ne peut être exercé qu'une fois tous les six mois et le responsable du traitement doit répondre dans les 30 jours suivant la demande.

Défis : Le prochain défi à relever pour la Pologne concerne le nouveau projet de loi du ministère des Affaires numérique qui accompagnera l'entrée en vigueur du règlement général de la protection des données de l'UE en Pologne. Une consultation publique devrait avoir lieu.