COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 28 June / juin 2018

T-PD(2018)12Mos

CONSULTATIVE COMMITTE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL

(Convention 108)

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

/

Information sur les developpements recents intervenus dans le domaine de la protection des donnees 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

INFORMATION AND DATA PROTECTION COMMISSIONER (IDP)
(Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale)
www.idp.al

REPORTING PERIOD (JUNE 2017- MAY 2018)

Complaints

Over **150** complaints have been lodged throughout this period, out of which **123** complaints were processed according to the Law "On the Protection of Personal Data"

For the equitable and full processing of complaints, administrative inspections were conducted with various controllers and all the administrative procedural steps were performed such as continuous communication with applicants and data controllers in order to obtain information.

The scope of processed complaints is related mainly to:

I. Violation of data subject rights (right to access, as a fundamental right of the data subject, allowing the latter to receive information by the controller regarding its data processing);
II. Lack of personal data security (data processing in network and online security);
III. Unfair and illegal data processing (dissemination in the media and online portals);
IV. Installing cameras in public and private areas;
V. Direct marketing regarding unsolicited communications, via phone or email;
VI. Exceeding the deadline of personal data collection for a specific purpose.

Large part of the complaints has been filed with the Commissioner's Office through email available to data subjects: info@idp.al, through our green number, or handed over personally after consultation with the communication officers. This year has also been made available a Smartphone app entitled "IDP Complaint", where citizens can directly lodge complaints with the Commissioner's Office.

Notification

During this period **133** data subjects have notified data processing, conforming thus to their legal obligation. The total number of controllers registered in the Central Register of Controllers amounts to **5455.**

Administrative investigations

The Commissioner's Office has carried out 132 on-site inspections mainly in Tirana, whereas 30 with public controllers and 102 with private controllers. Inspections have been initiated based on complaints (17), and *ex officio* (115).

Main sectors under scrutiny were:

- Health;
- Banking sector;
- Telecommunications, (process of personal data destruction);
- Direct marketing;
- Call centre
- Public and non-public higher education;
- Public and non-public social care institutions;
- Private physical security companies
- Institutions for execution of criminal decisions
- Non-profit organisations (NGO)
- Ministry of Health
- Ministry of Education
- Ministry of Justice
- Hotels
- Bailiffs
- Asset Evaluation Offices

It is important to emphasize the cooperation with the Italian Personal Data Protection Authority (Garante) in the framework of a joint inspection conducted with two controllers operating in the call centre sector in the territory of the Republic of Albania. The adopted procedure is a novelty to the Commissioner's Office due to the application of new techniques regarding the identification of processing procedures during telemarketing with Italian and Albanian clients throughout this inspection, which was assisted by Italian counterparts. The noticed issues are related to guaranteeing the rights of data subjects (consent and information), taking measures for ensuring the security and confidentiality of personal data processed via the telecommunications network, and guaranteeing the transfer of clients' data during international transfer.

The inspection of the project "*Identification and Population of the Address for Every Citizen*", during which several shortcomings regarding the project on-site implementation were noticed, was given priority. Commissioner's Office appreciates the controllers' willingness in cooperating and fulfilling their legal obligations in this area.

Upon conclusion of the administrative investigations, **46** hearing sessions were conducted, followed by the relevant acts rendered by the Commissioner's Office.

Recommendations / Orders

The Commissioner, in accordance with the competences conferred by Law No. 9887/2008 "On the Protection of Personal Data", as amended, has rendered **68** Recommendations for public and private controllers.
Additionally, the Commissioner has rendered **12** Orders "*On prohibiting data processing and further collection, and destroying immediately those data which have been illegally collected*" for public and private controllers.
Unifying standards in specific sectors
Based on the positive experience of the previous year, which was marked by the successful implementation of the Commissioner's Unifying Recommendations, the Commissioner has continued to provide recommendations of such nature in the following sectors:
Recommendation in the Tourism Sector
The Commissioner's Office appreciates the importance of this sector, and upholding confidentiality and data protection, in the frame of its impact on the life of any citizen and the importance of their personal data and privacy protection, due to the increase of mobility influxes at the local and international level of Albanian and alien citizens (in the capacity of data subjects), and electronic and manual processing of a large quantity of personal data by tourism agencies.
Recommendation for Institutions for Execution of Criminal Decisions
The Commissioner's Office has conducted administrative investigations with the Institutions for Execution of Criminal Decisions. The Commissioner's Office has come up with a recommendation for such institutions, depending on the violations noticed, as well as a recommendation for the General Directorate of Prisons as the superior body regarding the violations in I.E.C.D. The main issues noticed in such institutions are generally violations related to the quantity of data collected on employee subjects, inadequate measures on guaranteeing security, integrity, and availability of electronic data, computer equipment, operative systems, video surveillance systems (CCTV), lack of regulation for personal data processing, and declaration of confidentiality regarding the data that they access, etc.

Administrative Sanctions
After conducting administrative investigations with various public and private controllers ex officio or based on complaints, the Commissioner's Office has imposed sanctions with punitive fine in cases of serious and recurrent violations, or in case of failure to fulfil the Commissioner's recommendations/orders.
With reference to the figures of 2017, the Commissioner's Office has issued **22** decisions, which correspond to **36** administrative sanctions, whereas over the period January - May 2018, the Commissioner's Office has issued **4** decisions with punitive fine, which correspond to **5** administrative sanctions.

International transfer

Priority was given to the follow-up of personal data international transfer monitoring mainly in strategic sectors such as banking system and pharmaceutical industry, aiming to ensure a better protection of citizens' personal data.

In addition, based on the data obtained by the filled out Notification Forms and upon finding out that the transfer is taking place in countries with insufficient level of protection, additional information has been solicited from the controllers and the respective practices of transfers were subsequently examined.

5 decisions on permitting international transfer have been issued.

Co-operation/Meetings

In terms of strengthening professional capacities, was organised on 14-15 November 2017, in collaboration with TAIEX an expert mission on the Impact of General Data Protection Regulation in Acceding Countries. The mission mainly focused on the innovations provided by the EU General Data Protection Regulation and EU Directive No. 680/2016 in relation to the European legal landscape and its convergence in third parties. A second expert mission followed in February 2018 on the "Alignment of the Data protection Law with EU Data Protection Legislation". Beside IDP staff, the mission gathered also representatives of the People's Advocate and the General State Police.

The Office of Information and Data Protection Commissioner in co-operation with "Ernst & Young Albania" firm organized an event on "The Impact of EU General Data Protection Regulation on the Private Sector in Albania". The meeting aimed at informing and raising awareness regarding the additional obligations and rights that this Regulation shall introduce, not only in the EU Member States, but on a global scale. Furthermore, it pointed on the necessary steps that Albanian businesses companies must take in order to ensure compliance with the protection of personal data according to the applicable national legislation and the General Data Protection Regulation. The Office of the Commissioner and "Ernst & Young Albania" signed a Co-operation Agreement by medium of which Parties engage in exchanging experience and receive assistance in the process of alignment of national legislation on the protection of personal data with the relevant European legal framework.

Additionally, at the premises of the Commissioner's Office was held a training on the "EU General Data Protection Regulation" with keynotes from experts of "Ernst&Young"

Awareness-raising

The Office of Information and Data Protection Commissioner in cooperation with "Ismail Qemali" University of Vlora and with the support of OSCE presence in Albania, organized on 30 May – 2 June 2017, the "Information and Privacy" Summer School. This event aimed at raising awareness of citizens in upholding their right to privacy and the right to access official information. The 4 days of the training programme of the Summer School gathered over 100 students, academic and administrative staff of the University of Vlora.

IDP has continued providing training to the 9-year school staff regarding "Teachers' competency framework in the 9-year schools on the protection of pupils' personal data" in 8 different cities in Albania.

The Office of the Commissioner attended an event organised by the American Chamber of Commerce and the PwC Albania with focus on the EU General Data Protection Regulation (GDPR) and the compliance of public sector with its legal obligations.

The Office of the Commissioner attended the launching meeting of the "Internet Governance Forum in Albania" organised by the homonymous association. Internet Governance Forum is an initiative of civil society adopted by the United Nations and monitored by a special Secretariat (UN-IGF Secretariat). This initiative targets the co-operation of all stakeholders, both public and private to establish regulatory standards in this domain. This first meeting was held at the premises of COD Centre located at the Prime Minister's residence, and gathered representatives of the Electronic and Postal Communications Authority, the Ministry of Infrastructure and Energy, the National Authority for Electronic Certification and Cyber Security the UN Secretariat for Internet Governance, academia, civil society, various ICT companies, interest groups, media, etc.

A training seminar was held on 21-22 November 2017 in co-operation with the Academy of Security entitled "Information and Privacy". The event gathered academic and administrative staff from the State Police education institution. Certificates were distributed for the attendees.

The Office of the Information and Data Protection Commissioner, in collaboration with the Council of Europe organized the workshop "Safeguarding privacy in the media". This event was attended by representatives of central institutions, justice system, independent authorities, civil society, media etc. Local and international experts delivered presentations on privacy related issues with respect to the Media work and the European legislative reform in the field of personal data protection, with focus on the EU General Data Protection Regulation, the Police Directive and the modernization of Convention 108.

A cooperation agreement signed between IDP and the Mediterranean University preceded the Winter School, held on 25-26 January 2018, as part of activities organized by the Office in the Data Protection Week. The Winter School gathered 70 participants amidst students, academic and administrative staff of various universities. Attendees gain knowledge on the national legislation on the protection of personal data, implications of technology for privacy, European legislative landscape, the legislation on freedom of information, IoT, the research conducted by IDP "Privacy and security of personal data when using social networks from 15-18 age group" etc.

On January 28th, IDP introduced a postage stamp issued by the Albanian Post entitled "January 28 – data Protection Day". It was an initiative of the Commissioner's Office to mark 28 January, Data Protection Day. It represents all the elements included in the concept of the protection of privacy and in particular, the relation of individual with the technology.

IDP organised in the city of Korça a meeting entitled "Right to Information and Data Protection: introduction with relevant legal requirements" held in the framework of a cooperation Project with OSCE Presence in Albania. The focus of this event was to provide first hand information to the representatives of central institutions at local level, local self-government bodies, justice system, etc. on striking the right balance between both constitutional rights vis-à-vis their fields of activity.

Publications

The Office of the IDP Commissioner has also:

- Translated in Albanian the "Handbook on European Data Protection Law" authored FRA and the Council of Europe;
- Issued the 3rd edition of its Magazine "Information and Privacy";
- Issued several fliers on the occasion of its 10 years of establishment.

Conference of European Data Protection Authorities

"Data Protection – Better Together"
3-4 May, Tirana – Albania

The 28th edition of the Conference of European Data Protection Authorities (European Conference) was hosted by the Office of Information and Data Protection Commissioner (IDP) of Albania in Tirana, on 3-4 May 2018. The IDP Commissioner's Office prepared a dedicated website for the event which will remain active for at least several months after the event. The Conference brought together more than 95 delegates from over 46 data protection authorities and observers. It included 7 panels and several sessions, ranging from cooperation in intelligence oversight, territoriality of the GDPR, state of play for the revision of Convention 108, data protection in the context of police and justice bodies as well as in the Humanitarian Action, global influence of European standards and the latest revelations on micro-targeting and political campaigning in social media. Some updates on the activities of certain data protection networks were presented, such as the Francophone Association of Data Protection Authorities, Central and Eastern European DPAs and the Case Handling Workshop. An informal lunch discussion on the future of the International Conference (ICDPPC) was also held on the margins of the European Conference.

The Working Group on the Future of the European Conference led by the CNIL and coordinated by IDP introduced on the second day of the Conference a Discussion Paper, and taken note of members' inputs during the plenary. The Working Group was granted an extended mandate until the next edition of the European Conference to continue working on preparing a document containing a set of proposals, and further steps to be followed in order to determine the strategic goals of the Conference and clearly define the latter's mission and functioning. The Accreditation Committee of the European Conference submitted an Accreditation Report as well as a Resolution on the Accreditation of the Turkish Data Protection Authority as member of the Conference of European Data Protection Authorities. Some Members asked for more time to review these documents, therefore it was decided to postpone the decision to the next edition of the Conference. In addition, the Working Group on the Future of the ICDPPC held an informal lunch discussion on the future of the International Conference (ICDPPC) in the margins of the Conference of European Data Protection Authorities.

The IDP Commissioner's Office will remain member of the Accreditation and Support Committee of the European Conference until 2020.

International Conference of Data Protection and Privacy Commissioners (ICDPPC)

2019, Albania

The IDP Commissioner's Office will host the 41st International Conference of Data Protection and Privacy Commissioner (ICDPPC) in Tirana, Albania. The Commissioner's Office has already established a working group and set forth several objectives in terms of logistics, whereas close consultations are under way with counterpart authorities aimed at drawing the first lines of the draft programme of this major event. The period when the Conference should take place is between the last week of September and first two weeks of October 2019.

ANDORRA / ANDORRE

Développements majeurs survenus dans le domaine de la protection des données en **Andorre** depuis la *34ème réunion plénière qui s'est tenue en juin 2017*

Législation qui, dans des domaines spécifiques ou à des fins spécifiques, a créé, détaillé et développé des règles de protection des données à caractère personnel.

Loi 12/2017 du 22 de juin, sur la surveillance des assurances et reassurances
Sont soumis à la surveillance au sens de la présente loi: les entreprises d'assurance qui exercent une activité en matière d'assurance ou de réassurance en Andorre et les entreprises d'assurance ayant leur siège social à l'étranger, mais qui exerce leur activité en matière d'assurance en Andorre et son Règlement d'aplication du 20 décembre 2017.

Loi 16/2017 du 13 juillet sur l'hébergement touristique et les Règlements d'application du 2 mai 2018 relatifs au Registre d'hébergements touristiques (HUT) et d'entreprises de gestion des hébergements touristiques (EGHUT) et le Règlement sur le Registre d'ocupation d'hébergements touristiques (ROAT) qui précise les communications et les données qu'il doit contenir.

Loi 20/2017 du 27 octobre relative aux droits et devoirs des professionnels de la santé et le dossier médical. L'objectif de cette loi est de régler le droit à l'information des utilisateurs, les droits des professionnels de la santé, le dossier médical. Elle porte spécialement sur les conditions de l'utilisation des données nominatives dans les banques de données médicales, à des fins thérapeutiques et de recherche, ainsi que les modalités d'accès et de communication, consentement exprès du patient, les personnes mineures,...).

Loi 30/2017 du 30 novembre, de modification de la Loi 19/2016 sur l'échange automatique d'information en matière fiscale et où il s'avère que si un pays ne respecte pas ses obligations en matière de confidentialité et de protection des données, l'Andorre peut suspendre l'échange automatique de renseignements avec le pays concerné.

Activités de l'autorité de protection des données

Le rapport annuel de l'Agence Andorrane de protection de données détaille l'ensemble de ses activités. https://www.apda.ad

Un nombre sans cesse croissant de demandes de renseignements concernant les droits des personnes concernnées a conduit l'Agence à publier des lignes directrices à ce sujet .

ARGENTINA / ARGENTINE

Argentina News 2018

1) Changes in the institutional framework of the Argentine DPA

The National Personal Data Protection Directorate, dependent of the Ministry of Justice and Human Rights, was the argentine data protection authority responsible of guaranteeing information privacy at a national level, in accordance with federal Law Nº 25.326. As from September 2017, the Access to Public Information Agency, autarchic and autonomous entity created by law in 2016, has become the argentine data protection authority as well as the public information agency (Decree Nº 746/2017 and Nº 899/2017).

As a result of this legislative change, the data protection authority has gained independence, a key element for the protection of personal data according to international standards. In this sense, under the new regulation, the Agency's Director is appointed by the President and shall be dismissed only with the approval of the National Congress and only in case of ill performance of his/her duties. This procedure contrasts to the previous one in which the Director was designated and dismissed by the Minister of Justice and Human Rights. Additionally, under the new regulation, the Access to Public Information Agency has its own annual budget, in contrast to the previous data protection authority.

- 2) Argentina invited to accede Convention 108).

On September 27th,2017 the Committee of Ministers agreed to the request of Argentina to be invited to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol regarding supervisory authorities and transborder data flows. In March 2018, the Executive branch submitted to the National Congress a draft bill for the approval of Convention 108 and its Additional Protocol. The Access to Public Information Agency's Director actively participated in two sessions addressed by the Congress' Commission for Foreign Affairs. As a result of these sessions, the Commission submitted a legal opinion recommending the approval of Convention 108 and its Additional Protocol on April 18th. However, its debate by the Senate is still pending.

- 3) Draft bill elaborated by the Argentine Data Protection Authority in 2016-2017. Technological changes that have taken place during the last seventeen years as from the enactment of the Argentina's Data Protection Law together with the new international legal context, principally with the enactment of the EU Data Protection Regulation (GDPR (EU) 2016/679), regulation that has recently become enforceable, have driven the Argentine Data Protection Authority to elaborate in 2016 a draft bill to reform the current law. The draft bill is intended to provide a high level of protection of personal data and, at the same time, bring new possibilities of innovation and investment in Argentina. In 2017, Argentina's President, Mauricio Macri, announced at the Opening Session of the National Congress that this draft bill would be submitted to the Congress. The draft bill is still under study of the Executive branch and has yet not been submitted to the Congress.

AUSTRIA / AUTRICHE

Major developments in the data protection field in Austria:

- A GDPR implementation law was passed in July 2017 and was amended in April 2018
- The Head of the Austrian Data Protection Authority was elected as Chair of the Working Party 29 in February 2018 and elected as Chair of the European Data Protection Board on the 25th of May 2018

BELGIUM / BELGIQUE

- Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, laquelle réforme complètement l'autorité de contrôle afin de lui attribuer les compétences RGPD notamment.

- Avant-projet de loi relative à la protection des données à caractère personnel qui doit remplacer la loi actuelle vie privée du 6 décembre 1992. L'objectif de cette loi est de prévoir des mesures d'exécution du RGPD, transposer la directive 2016/680 pour la police/justice, et prévoir les dispositions de la Convention 108 pour les services de renseignements. L'avant-projet de loi a été approuvé par le Gouvernement, il est actuellement en discussion au Parlement.

- Une série de législations sont modernisées et adaptées au nouveau RGPD.

BOSNIA AND HERZEGOVINA / BOSNIE ET HERZEGOVINE

Subject: **Major developments in the data protection field in Bosnia and Herzegovina for the period June 2017 – May 2018**

The Agency for Personal Data Protection in Bosnia and Herzegovina was established by the Law on Personal Data Protection (Official Gazette of BiH, No. 49/06) and started its work in June 2008. The Law on Amendments to the Law on Personal Data Protection ("Official Gazette of BiH" No. 76/11) was adopted by the Parliamentary Assembly of Bosnia and Herzegovina in 2011. The Rulebook on Internal Organization and job classification provide 45 working positions in the Agency. Currently, 25 employees are employed in the Agency.

Normative part

One of the legal obligations of the Agency is to monitor the situation in the field of personal data protection and to give proposals, initiatives and opinions in this regard. During the reporting period, the Agency prepared 38 opinions and one response to various proposals of laws and other administrative acts, as follows:
To the Ministry of Justice of BiH on the Draft Law on Amendments to the Law on Ministries and Other Bodies of the BiH Administration, the House of Peoples of the Parliamentary Assembly of BiH (PA of BiH) on the Proposal of the Law on Amendments to the Law on Administration, the Ministry of Justice of BiH on the Draft Law on Amendments to the Law on Salaries and other Remuneration in Judicial and Prosecutorial Institutions at BiH level, the House of Peoples of the PA of BiH on the Proposal of the Law on Parliamentary Control, the Ministry of Security of BiH on the Draft Grounds for Negotiating and Concluding the Draft of the Agreement between the European Union and BiH on Border Cooperation, the Ministry of Communication and Transport of BiH to the Draft Law on Amendments to the Law on Communications, the House of Peoples of the PA BiH on the Proposal of the Law on Amendments to the Law on Administrative Fees, the Ministry of Communication and Transport of BiH on the Draft Law on Electronic Communications, the House of Peoples of the PA of BiH on the Proposal of the Law on Public Broadcasting System of BiH, the Indirect Taxation Authority of BiH (ITA BiH) to the Draft Law on Amendments to the Law on ITA, the Ministry of Human Rights of BiH on the Proposal of the Law on Amendments to the Law on Human Rights Ombusman of BiH, House of Peoples of the PA of BiH on the Proposal of the Law on Amendments to the Law on the Basis of Traffic Safety on Roads in BiH, the House of Peoples of the PA of BiH on the Proposal of the Law on Amendments to the Civil Service Law in BiH Institutions, the House of Peoples of the PA of BiH on the proposal of the Law on Amendments to the Election Law of BiH, the House of Peoples of the PA of BiH on the Proposal of the Law on Amendments to the Law on Independent and Supervisory Bodies of the Police Structure in BiH, the Ministry of Human Rights and Refugees BiH regarding the request for an opinion on the draft Rulebook on the procedure of registration, content and manner of keeping records of associations and alliance of emigrants from BiH, the Deposit Insurance Agency of BiH on the Proposal of the Law on Deposit Insurance in Banks of BiH, the Ministry of Veterans Affairs of HNK regarding the submitted preliminary Draft Law on Additional Rights of Veterans and Members of their Families in the HN Canton, the Ministry of Justice of BiH to the Draft Law on Amendments to the Law on Administrative Disputes of BiH, the House of Peoples of the PA of BiH on the Proposal of the Law Amending the Law on Amendments to the Law on Salaries and other Remuneration in Judicial and Prosecutorial Institutions at the BiH level, the Ministry of Justice of BiH to the Draft Law on Amendments to the Labor Law in the Institutions of BiH, the Council of Ministers of BiH on the Proposal of the Law on Amendments to the Law on Excises in BiH, to the Draft Law on Amendments to the Law on Passing the Bar Exam in BiH, the State Secretary for Public Policy and Political Initiatives of the SDP BiH on the Proposal for Amendments to the BiH Election Law, the Ministry of Communications and Transport of BiH was given an opinion to the Draft Law on Electronic Identification and Trust Services for Electronic Transactions, to the Draft Law on the Rights of Victims of Torture in BiH, the PA of BiH - The House of Representatives, on the Proposal of the Law Amending the Criminal Code of BiH, the Ministry of Defense of BiH on the Proposal of the Law on Amendments to the Law on Service in the Armed Forces of BiH, the Federal Ministry for the issues of Veterans and Disabled Veterans of Liberation War was given an opinion on the Proposal of the Rulebook on the establishment of a Single

Register of Veterans and Users of Rights in the field of Veteran Disability Protection to the Ministry of Security of BiH on the Draft Law on Police Officers of BiH, the Ministry of Security of BiH on the Proposal of the Law on the State Investigation and Protection Agency, the Ministry of Finance and Treasury of BiH on the Draft Law on Amendments to the Law on Financing of Institutions of BiH, to the Draft Law on Amendments to the Criminal Procedure Code of BiH, the Draft Law on Amendments to the Law on Misdemeanors, the House of Peoples of the PA of BiH on the Proposal of the Law on Amendments to the Law on Salaries and Remunerations in the Institutions of BiH, to the House of Representatives of PA of BiH on the Proposal of the Law on Amendments to the Law on Amendments to the Law on Aviation of BiH, the Ministry of Finance of the Republic of Srpska on the text of the Law on Amendments to the Law on Internal Payment Transactions, the House of Representatives of PA of BiH on the Proposal of the Law on Amendments to the Election Law of BiH, the Ministry of Communications and Transport of BiH on the Draft Agreement between the Council of Ministers of BiH and the Government of the Republic of Malta on mutual admission and replacement of driving licenses, the Ministry of Communications and Transport of BiH to the Draft Law on Aviation of BiH, the House of Peoples of the PA of BiH on the Proposal of the Law on Amendments to the Law on Protection of Persons Reporting Corruption in the Institutions of BiH, the House of Peoples of the PA of BiH on the Proposal of the Law on Amendments to the Labor Law in the Institutions of BiH, the House of Representatives of PA of BiH on the Proposal of the Law on Amendments to the Law on Salaries and Remunerations in the institutions of BiH, the Ministry of Civil Affairs of BiH on the Proposal of the Law on Amendments to the Law on Sports in BiH, the Ministry of Civil Affairs of BiH on the Proposal of the Law on Amendments to the Law on Demining in BiH.

Providing expert opinions on the requirements of the controllers and personal data subjects is constantly increasing. The large number of requests for opinions by public and private sector testifies increasing awareness of all entities regarding personal data protection. 189 expert opinions on public and private sector requests, 130 responses instead of expert opinions, 10 opinions on personal data transfer abroad and 3 responses to the requests of natural and legal persons were provided.

Through the inspection, the Agency supervises the fulfillment of the obligations prescribed by the Law on Personal Data Protection. In carrying out its regular monitoring activities, the Agency performed 48 regular and 32 extraordinary inspection controls during the reporting period and passed 49 decisions and 2 conclusions upon regular inspections performed.

During the reporting period, 4 judgments of the Court of BiH were adopted in favor of the Agency, 17 responses to the lawsuit were submitted and 2 requests for review of the court decision were made.
According to the activities of the Agency carried out during the reporting period, the state of protection of personal data in our country could be described as satisfactory. It is important to emphasize the increase of the number of complaints filed by citizens, which indicates an increase in awareness of the importance of protecting personal data. In the reporting period, 74 decisions were made upon complaints, mostly against public bodies, but also other controllers, business entities and natural persons. 110 activities were carried out in the resolving complaints procedure. The Agency started issuing misdemeanour orders in 2011, and during the reporting period, 10 misdemeanour orders were issued.

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

Cooperation with the media

The Agency regularly informs the media about its competencies and activities, promotes the work of the Agency and informs the public about the processing and protection of personal data. The Agency regularly responded and reported on all queries of the media through all available means of public information and by publishing opinions and decisions on the official website of the Agency, as well as through the Help desk.

Regarding the above, a press conference was held on the occasion of marking the European Data Protection Day 28 January 2018. There were 16 written responses, 12 statements and 8 visits to the media on various inquiries of print and electronic media. Through the Help Desk of the Agency, 383 inquiries of citizens were answered.

The website of the Agency is regularly updated with the necessary content, which shows the commitment to transparent operation of the Agency. During the reporting period, 50.481 visits to the homepage of the Main Registry on the Agency's website were recorded. There were 124 posts related to the activities and work of the Agency and the protection of personal data in the media and on the Internet. Also, there were 124 posts in the media and on the Internet related to the activities and work of the Agency and the protection of personal data.

At the initiative of the Sector for International Cooperation and Public Relations, in May 2017, the application procedure for the **TAIEX Expert Mission in the Agency for the Protection of Personal Data in BiH** was launched.
The aim of the Expert Mission was to harmonize the Law on Personal Data Protection of in BiH with the Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and on the repealing of Directive 95/46/EC (General Data Protection Regulation). The Agency suggested the EU experts from the Agency for Personal Data Protection of the Republic of Croatia and from the Saxon Data Protection Commissioner. It was suggested for the expert mission to be held in October 2017.
The TAIEX expert mission was realized in October 9-14, 2017, and the European Union experts were Bernhard Bannasch, Deputy Saxon Data Protection Commissioner of Germany and Sanja Silaj Zeman, Head of Department for International Cooperation, EU and Legal Affairs from Croatian Agency for Personal Data Protection. Participants of the event were representatives of the Agency for Personal Data Protection in BiH, the representative of the Directorate for European Integration of the CM BiH, the representative of the Delegation of the European Union to BiH, and the guests from the Republic of Serbia Mr. Rodoljub Sabic, the Commissioner for Information of Public Importance and Personal Data Protection and Mr. Marinko Radic, Secretary General of the Commissioner's Office. In five working days, EU experts held a series of lectures, presenting to a certain extent the application of the provisions of that Regulation, and together with other participants considered important steps in drafting a new Law on Personal Data Protection, and establishing standards for the protection of personal data in Bosnia and Herzegovina, modeled on the member states of the European Union.

Due to the complexity of the process of harmonization of legislation, the Agency planned to continue the cooperation with the aforementioned experts from the EU in the form of a **Study Visit to the Saxon Data Protection Commissioner in Dresden (Germany)** and the Croatian Agency for Personal Data Protection at the beginning of 2018. Representatives of the Agency would thus have the opportunity to get acquainted with the experiences and best practices regarding the transmission and application of the latest standards for the protection of personal data generated by the implementation of the provisions of the General Data Protection Regulation in the Federal Republic of Germany and the Republic of Croatia.
According to the request of the TAIEX office, forms for the participation of three representatives of the Agency were filled in and submitted. Since two study visits can not be approved by one application, it is suggested that this Study Visit would be to the Saxon Data Protection Commissioner. The aim of the study visit is the need to harmonize the Law on Personal Data Protection in BiH with the General Data Protection Regulation. The primary plan was to realize the Study Visit in the second half of January 2018. The suggested term in January was shifted to in April 2018 by the TAIEX Office, and, following the current and immediate obligations related to the application of GDPR, the Saxon Commissioner proposed the study visit for September/October 2018.

In accordance with the planned activities of the Agency, to strengthen public awareness of the protection of personal data and privacy, activities on the creation and realization of the Project for education of children in elementary schools in Bosnia and Herzegovina "Do not leave your tracks on the Internet" started in 2017.
The aim of the Project is to introduce children the way in which they exercise and protect their rights and interests on the Internet, raising awareness about the importance of protecting personal data and privacy in the digital world, and contributing to greater security of children on the Internet.
By analyzing the Curriculum of nine year primary schools in Bosnia and Herzegovina, it was found that students listen to the informatics subject for the first time in the VI grade of primary school. For that reason, the Project proposal was to hold lectures on the protection of personal data on the Internet for VI classes of a certain elementary school, within one or two school classes of Informatics.

Until May 15 2018, the project was implemented in 22 towns in Bosnia and Herzegovina. In 27 primary schools, 1898 students attended the lecture. By the end of the school year 2017/2018, more lectures in elementary schools in Canton Sarajevo are planned.

Director
Petar Kovačević

BURKINA FASO

Voici les grandes évolution en matière de protection des données personnelles au niveau du Burkina Faso depuis 2017:

1- la poursuite du processus de relecture de la loi 01-2004/AN du 20 avril 2004 portant protection des données personnelles. L'avant-projet de loi n'attend que le quitus du Conseil des Ministres pour transmission à l'Assemblée nationale pour adoption.

2- La Commission a également connu le renouvellement de ses membres au cours de l'année 2018 après la fin de mandat de quatre (04) Commissaires en fin 2017

3- La CIL a été portée à la tête du Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP) en février 2018 et sa Présidente élue membre du Comité exécutif de la Conférence internationale en septembre 2017.

CAP VERT / CAPE VERDE

Activités menées depuis juin 2017

Au cours des douze derniers mois, la Commission Nationale de Protection des Données à Caractère Personnel (CNPD) a tenu plusieurs conférences destinées aux institutions publiques, entreprises publiques et privées, associations communautaires, avec comme objectif une divulgation de la loi de la protection des données à caractère personnel et une sensibilisation sur les défis en matière de sûreté de l'information.

Il convient de souligner la protection des données relatives à la santé dont le thème, en plusieurs occasions a été abordé avec les médecins des hôpitaux centraux de même qu'avec l'Ordre des médecins.

Pour marquer la Journée Européenne de Protection des données à caractère personnel, la CNPD a réalisé des conférences sur la protection des données à caractère personnel dans deux Ecoles Secondaires.

La CNPD, en partenariat avec le service de contrôle économique, a réalisé plusieurs actions de formation pour les inspecteurs des Mairies.

Pour la première fois au Cabo Verde, la CNPD a donné son avis sur l'installation du système de vidéosurveillance dans l'espace public pour la sécurité urbaine, en faisant des recommandations visant au respect des droits à la protection de l'intimité de la vie privée et familiale ainsi qu'à la protection des données à caractère personnel.

La CNPD a également réalisé, le 19 avril 2018, une conférence sur le thème " Privacité et Vidéosurveillance dans l'espace public". Cet événement dont la cérémonie d'ouverture s'est tenue sous la présidence du Président du Parlement caboverdien, a enregistré environ 150 participants et a été une occasion pour un débat sur les libertés fondamentales concernées ainsi que les enjeux globaux relatifs à la vie privée et le rôle de la CNPD en tant qu'autorité de contrôle.
A la même date, la CNPD a signé un protocole avec la Police Nationale, dans lequel il a été convenu un programme de formation en vue de la réalisation d'activités de contrôle en matière de traitement de données à caractère personnel à la sollicitation de la CNPD.

La CNPD a approuvé les orientations générales applicables aux traitements des données à caractère personnel résultant du contrôle de l'utilisation, à des fins personnelles, des technologies de l'information et de la communication (téléphone fixe et/ou portable, Internet et courrier électronique) dans le cadre du travail.

Sous l'impulsion de la CNPD, l'Assemblée Nationale du Cabo Verde a approuvé, par ratification, le 28 juin 2017, la Convention n°108 pour la Protection des Personnes relativement au traitement automatisé des Données à Caractère Personnel ainsi que les amendements supplémentaires. Son Excellence le Président de la République a ratifié la Convention n°108 en février et il ne reste que le dépôt de cet instrument.

Accordant une attention particulière aux pays d'expression portugaise, les membres de la CNPD ont rendu visite aux services du Cabinet de Protection des Données à Caractère Personnel (GPDP) de la Région Administrative Spéciale de Macau. A cette occasion, les deux entités ont partagé leurs expériences et se sont engagées à mener des actions de coopération à l'avenir.
Consciente du fait que la protection des données à caractère personnel est un facteur de développement économique et social en Afrique et de la nécessité d'un cadre de coopération et de collaboration entre les différentes autorités de protection, la CNPD a participé à l'assemblée générale du Réseau Africain des Données qui s'est tenue à Casablanca, au Maroc, le 23 février 2018. Et à ce forum, la CNPD a été élue deuxieme vice-présidente.

CNPD, 30 juin 2018
Praia, Cabo Verde

CYPRUS / CHIPRE

Major developments in the data protection field

EU's General Data Protection Regulation (GDPR)

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, is applicable since 25 May 2018. The draft law on the implementation of certain provisions of the Regulation is currently discussed at the Parliament and should be adopted shortly.

The Commissioner for Personal Data Protection has put significant investment into raising awareness and preparing for the GDPR. The awareness campaign comprised conferences and speaking events, media engagement, information campaigns and the development of a new website.

Namely, over the year before the application of the GDPR, the Commissioner delivered presentations and speeches in more than fifty institutions and organisations. Moreover, one thousand DPOs from the private and public sector received training.

Despite these actions, awareness level needs to be reinforced and it is commonly acknowledged that many organisations, both in the public and private sector, must pursue their engagements in order to be fully complied with the GDPR.

The Commissioner has asked for significant budget and staff increases. Decision has been taken by the Ministry of Finance to increase the staff by three officers in order to comply with its future functions and principal activities of the DPA. However, to date, this engagement has not been materialised, thus jeopardising the ability of the DPA to effectively perform its tasks and exercise its powers in accordance with the GDPR and FOI act.

Law regulating the right of access to public sector information (FOI)

The law regulating the right of citizens to access public sector documents and information was adopted in December 2017 and it will be applied in December 2018. 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.

Guidelines and decisions issued by the Commissioner

Guidelines on setting a retention period in the banking sector and the medical sector
The lack of coherence between policies on the retention period of data processed by financial institutions demonstrated the need of uniformly adjusting the retention period of data held by financial institutions. Following a consultation and exchange of views on the matter, in particular with the Cyprus Banking Association, and after taking into account to a large extent the Association's views and concerns as well as all the relevant legislation which impose an obligation to keep the data for specific periods of time, the Commissioner issued guidelines on the retention period.

The retention period in the banking sector was set for maximum 10 years after the last operation. The guidelines are legally binding

In the medical sector the retention period was set 15 years.

Guidelines on political direct marketing
The guidelines set out the legal requirements to be afforded by candidates and political parties, when processing personal data potential supporters for direct marketing purposes. According to the guidelines,

consent should cover all processing activities carried out for these purpose, including when political parties process data of their members/ supporters.

Fine imposed to a Credit Reference Agency (CRA)

The Commissioner imposed a fine of €25,000 to a CRA for unlawful processing of personal data. The CRA held databases of arrears and defaults payments on products which were offered to consumers and businesses. This included default payments in various sectors such as credit card facilities, telephone bills and insurance contracts.

The fine was imposed following a two-year investigation which revealed that the company was processing personal data unfairly and unlawfully and in contravention of the rules set out by the Commissioner.

A warning with a three-month deadline was further imposed to the company, in order to be fully complied with the GDPR. This includes the development of high level principles of data protection, security measures, the effective application of the provisions related to the processor, carrying out personal data impact assessments where necessary and the development of procedures enabling data subjects to exercise their rights.

Fines imposed for unsolicited electronic communications (sms and emails)

During the campaign for the Presidential elections of January 2018, the DPA received hundreds of complaints regarding unsolicited electronic communications, mainly text messages sent on mobile phones. The Commissioner issued warnings and imposed several fines for a total amount of circa €60,000.

CHILE / CHILI

Chilean Transparency Council
Data Protection Report 2018
DJ/UNR/12/06/2018

I. Legislative area

At the legislative level, efforts have materialized in the discussion of the following bills:

a) Bill N° 9.384-07. Enshrines the right to protect personal data

During 2017, the Executive granted legislative urgency to the Bill that constitutionally recognizes the fundamental right to protect Personal Data. The bill was approved by Congress and is currently awaiting promulgation by the President of the Republic.

b) Bill N° 11.144-07. Creates the Personal Data Protection Agency

In March 2017, the bill that seeks to regulate the protection and treatment of personal data and to create the Personal Data Protection Agency is presented. The bill aims to regulate the processing of personal data in order to ensure respect and protection of rights and freedoms of physical persons and in particular, the right for private life. It also creates the Personal Data Protection Agency as the supervisory authority in the matter.
It is currently in first stage of the legislative proceedings, awaiting to be discussed at the Constitutional Commission of the Senate.

II. Initiatives developed by the Chilean Transparency Council

a) Data protection week

During 2017, the Chilean Transparency Council, in its commitment to raise awareness in this subject, organized the Data Protection Week. Activities were focused on citizens, public officials and the Council's personnel. The event had the aim to cover, in the most comprehensive way, all the aspects needed to advance in improving standards and practices, as well as to disseminate and promote this right. Among others, the following initiatives were carried out by the Council:

- **A social network campaign called #CuidaTusDatos ("Protect your Data"),** with videos and infographics, in order to bring the public closer to the issue and to raise awareness of it.
- **A specialized website** (http://www.cuidatusdatos.cplt.cl), to familiarize and teach aspects related to protection of personal data.
- **Training for the Chilean Transparency Council's personnel** on comparative law, with a focus on the internship carried out by officials of the Council at the Spanish Agency for Data Protection. The training was meant to transmit the knowledge and experience acquired in the institution.
- **Training of public officials in protection of personal data**, with special emphasis on jurisprudence of the Chilean Transparency Council and of Chilean Courts of Justice, in aspects related to public health, labour and educational background, among others.

b) XV Ibero-American Meeting on Data Protection (June 2017)

During June, the XV Ibero-American Meeting on Data Protection took place in Santiago. It was attended by representatives, delegations and experts from 11 countries, and organized by the Chilean Transparency Council and the Ibero-American Data Protection Network. Participants **debated on how to advance in the safeguard and guarantee of private information when it is confronted to** massive collection of personal data.

The meeting addressed topics such as the right to be forgotten and the use of security cameras, drones and other videosurveillance devices, with almost no legal regulation in Chile.

Big Data was another of the axes of discussion promoted by the Council: **Which rights could be demanded by citizens when confronted to massive collection and processing of their personal data?**

The XV Ibero-American Meeting on Data Protection considered the participation of Congressmen, public officials, representatives of private companies and experts from organizations such as the Spanish Agency for Data Protection, the National Data Protection Authority of Argentina and international companies such as Google, Facebook, Microsoft and HP.

The meeting was the venue for the **approval and presentation of the Personal Data Protection Standards for Ibero-American States**. The guidelines were agreed among the members of the Ibero-American Data Protection Network, according with the new European data protection regulation, and with the highest international standards in the field.

c) Normative guidelines regarding the installation of video surveillance devices by municipalities

In 2017, the Chilean Transparency Council, in attention to the implementation of video surveillance devices through different technological mechanisms, such as surveillance cameras, hot air balloons, drones or any other instrument suitable for recording images for municipal security purposes, published Normative Guidelines with recommendations to local governments, to protect and secure personal data of the individuals. The Guidelines address the conditions, safeguards and responsibilities that should be adopted.

d) Campaign on national media on issues related to the protection of personal data

The Chilean Transparency Council took a strategic approach to communicate, through national media, on several issues concerning data protection. The media campaign sought to spread awareness regarding the processing of personal data in everyday situations. The Council promoted news pieces on the following topics:

- **Processing of personal data from the national identification number** (“RUT” in Chile). The “RUT” number is frequently solicited at commercial stores as a way to promote discounts and other benefits. However, the public is not fully informed of their rights under the law regarding the protection of their personal data. Hence, the Council took steps to explain how pharmacies, supermarkets and retail stores use the information of consumers when it comes to the collection of the “RUT” number.
- **Use of mobile applications**. The Council has frequently explained through the media which type of data information apps are collecting and processing. Also, it has informed about the importance of the privacy policies and the knowledge needed before installing any application or how to adjust privacy settings.
- **Safe navigation**. The Council explained how “surfing” on the web collects personal data and how security measures can be adopted in order to safeguard their data.

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

Latest developments in personal data protection
In the Czech Republic

The activities were mainly focused on the implementation of the new EU regulatory framework, if with a certain delay.

The Office for Personal Data Protection of the Czech Republic (hereinafter “the Office”) has been following as soon as since 1 January 2013 assessment of impacts on privacy and personal data protection. Unfortunately, even after for years of practical experience, the results yielded are not optimal. Some resorts repeatedly and untruly declare that their “processing of personal data will not interfere with the protection of privacy”.

One of the most important drafts, which the Office commented on, is the project of the act on population census foreseen for 2021. The project is based on a maximum use of the existing administrative sources of data as well as on a minimum burden for respondents because the data shall primarily be collected on-line. The Office brought forward comments concerning the specification of personal data and of further use of these data.

ESTONIA / ESTONIE

Major developments in the data protection field in Estonia 2017/2018

1. Legislation

Cybersecurity Act transposing the the Directive on security of network and information systems (NIS Directive) was adopted by the Parliament. This Act provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.

2. Relevant cases

2.1 *Estonia will have an artificial intelligence strategy.*

The Government Office and the Ministry of Economic Affairs and Communications has launched a cross-sectoral project to analyse and prepare the implementation of artificial intelligences, as well as develop a test environment in Estonia.

The expert group will prepare a draft law to allow the use of fully autonomous information systems, in all areas of life and to ensure the clarity of the legal area as well as required supervision.

The expert group will also develop an artificial intelligence strategy for Estonia covering both the public and private sector.

The working group will present the results by April 2019.

2.2. *Report on self-driving vehicles on Estonian roads.*

The expert group, instructed by the Strategy Unit of the Government Office, has issued its final report on self-driving vehicles, in which it broadly explains the potential, risks and possibilities involved in the digitalisation of traffic and self-driving vehicles. The report also looks at how 90% of the kilometres covered in Estonia could be self-driven by 2030 and what such a radical change would mean to the public sector, business and society.

The expert group's final report notes that success in implementing the change will depend on a change in attitudes and strategic steps taken at the state level, and the necessary investments in a new type of transportation infrastructure. The topic of self-driving vehicles must also be examined as a whole – with political, societal and legal questions being resolved alongside technological ones. Estonian Data Protection Inspectorate consulted working group on privacy and data protection risks.

As of March 2017, the testing of self-driving vehicles is legal on all public roads across Estonia. This is only permitted if a human driver is able to control the vehicle and thereby be legally responsible.

Report is available here (in Estonian only).

June, 12 2018

Annual Report 2017

Data Protection Ombudsman’s annual review

The Office of the Data Protection Ombudsman started its operations on 1 November 1987. Finland’s first act on the protection of personal data, the Personal Data File Act, entered into force on 1 January 1988. Finland celebrated its centennial of independence.

Operating environment

One of the key national and, in some respects, international themes of the reporting year was society’s ability to react to new threats. Finland experienced its first terrorist attack. The new reality was also reflected in global hacker attacks and blackmail (e.g. WannaCry, Petja), but also in the form of massive data leaks. Our own national scandal was caused by a story published by Helsingin Sanomat on the Finnish Defence Force's Viestikoekeskus (Signals Test Centre). The story was clearly linked to the gov-ernment proposals on intelligence operations presented to Parliament in 2017. According to a survey carried out by Lännen Media, citizens did not trust the authorities’ ability to protect sensitive personal data. The leak of data pertaining to the health status of 6,000 persons by an authority certainly did not reinforce trust in this vital task.

Society also reacted to increased threats in this area. The European Union restarted the planning of an overall architecture for the currently fragmented information systems based on different security instruments. The supervision of Europol was also subject to an overhaul. Questions related to double citizenships necessitated the amendment of the Security Clearance Act (726/2014). The Evaluation Criteria Committee established under the Act issued recommendations on the interpretation of criminal records.

Together with the Minister of the Interior, we launched a horizontal project for identifying bottlenecks in data flows in the Ministry's administrative branch and extending to the remits of different ministries. The work is slated to be completed this year.

Legislative work

A significant amount of legislative work took place in the reporting year. The Data Protection Ombuds-man was heard 59 times by Parliament on various bills. The TATTI working group instituted by the Minis-try of Justice delivered its report on the national data protection act. After the report, the working group continued preparing the alignment of Finland's exceptionally extensive special legislation with the EU's General Data Protection Regulation (2016/679). The report left open questions such as the national age limit for minority to be applied to the use of information society services, subjecting authorities to administrative sanctions and the relationship to the principle of openness. The officials of the Ministry of Jus-tice continued the preparation of the national data protection act, and a government proposal on the act was issued in early March 2018 (HE 9/2018 vp).

The working group on the development of information management (TILKE), instituted by the Ministry of Finance, published its report on 29 September 2017. Renewing the legislation on the protection of personal data by the Finnish Defence Force highlighted the challenges of reconciling our Constitution, the General Data Protection Regulation and the Data Protection Directive. For its internal use, the Office of the Data Protection Ombudsman drew up specific guidelines for evaluating government proposals from the perspective of the protection of personal data.

The work for the amendment of Finland's special legislation was begun in several administrative branches. Especially the work of the working group for the renewal of the personal identity code, instituted by the Ministry of Finance, caused much discussion. The Confederation of Finnish Industries even proposed giving every Finnish person a business ID at birth!

Excessive indebtedness once again featured in the headlines. The Minister of Justice held a discussion on the matter, which led to the appointment of a one-man committee to address the issue. Among other things, the committee was tasked with evaluating the registration and use of positive credit references. Only time will tell whether the discussion will eventually branch into the subject of using the approved Incomes Register (HE 134/2017) for the management of financial risks. The PSD2 directive is also related to the management of financial information and brings the crucial perspective of MyData into the discussion.

Preparing for the GDPR and Directive

As a matter of course, preparing for the adoption of the General Data Protection Regulation was one of the most important themes of the year. We decided that our Office's internal TSAU project primarily concerns competence management, and we will bring our organisation into line with the requirements of the GDPR at a later date.

According to the Yritysten rikosturvallisuus 2017 (Crime and Corporate Security 2017) report, 40% of Finnish companies had not made preparations for the GDPR. At the same time, it seemed that the offering of consultancy and expert services had increased significantly. Responding to the, frequently incorrect, news related to the GDPR was a major challenge for our Office. The regulation was overwhelmingly presented in terms of threats and sanctions, while we sought to highlight the opportunities for promoting the rights of data subjects and supporting the growth of the digital single market. Our communications were hindered by the fact that WP29 was responsible for the interpretation of the regulation and the guidelines on it.

The process of drawing up the guidelines took a surprising amount of time and the Office's resources. In the normal course of the process, WP29 first held a hearing on each theme with representatives of European industrial umbrella organisations. These organisations consulted their own networks when formulating their opinions. The matter was then referred to the sub-committee in charge of the particular area, which reported its proposal for the guideline to the steering group of data protection ombudsmen. After being discussed by the steering group, the matter was referred to WP29 for decision. The guidelines were then published for comment and updated by the WP29 if necessary. Finally, the Commission was able to start the translation of the guidelines into all of the EU's official languages. We communicated on the preparations of the guidelines on our website and at various events.

In accordance with our strategy, we were closely involved with the design and implementation of the training offered to Data Protection Officers. The cooperation project organised by Vahti and Juhta for the production of training and competence testing materials merits special thanks. The download amounts of the Arjentietosuojaa.fi videos exceed all expectations.

We would also like to thank the data protection forums organised by the Ministry of Transport and Communications for sharing competencies between the private and public sectors.

International matters

The Office's international cooperation increased in the reporting year. The work of establishing the European Data Protection Board was begun in Europe. We participated in the work of WP29 and its subcommittees actively, in which communications on European cooperation played a major role. Nordic cooperation also helped all parties in preparing for the implementation of the GDPR.

Phenomena and events

The year’s catchphrases were artificial intelligence, machine learning, robotics and block chains. The Ministry of Economic Affairs and Employment published a report titled ”Finland's Age of Artificial Intelligence”. The report set the objective of making our 100-year-old country a leading nation in the applica-tion of artificial intelligence. We were pleased to note that the report also addressed “AI” from a legal and ethical standpoint. The Ministry of Finance, on the other hand, published an article titled ”Finland needs information policy” to launch discussion on the subject. Data protection was placed high on the public agenda in 2017. In its way, the copyright letters case also touched on the protection of personal data.

In conclusion

The personnel of the Office of the Data Protection Ombudsman studied the GDPR, international working methods and its new duties, all the while bearing the burden of its daily duties. A strong commitment to defending the legal quality of life of Finland's citizens and providing proactive assistance to authorities and organisations helped us make it through the challenging year with our feet still dry. We will neverthe-less need a considerable boost to the Office’s resources in the coming years.

My heartfelt thanks to my colleagues!

Reijo Aarnio Data Protection Ombudsman

GEORGIA / GEORGIE

Office of the Personal Data Protection Inspector

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD

June 2017 – June 2018

GEORGIA

INCREASED PUBLIC INTEREST TOWARDS PRIVACY

Georgia is witnessing increased public interest towards privacy. Proved by the results of a nationwide survey commissioned by the EU and the UNDP in 2017, 81% of Georgian citizens consider data protection as a very important issue. The survey also showed that 2/3 of respondents think the state shall not intrude into their privacy, even for the purpose of ensuring security. The public's interest is also confirmed by growing numbers of complaints and consultation requests submitted by the citizens to the Office of the Personal Data Protection Inspector of Georgia ("**the Office**").

MAJOR ACTIVITIES OF THE DPA

The Office continues to carry out its functions and promote data protection standards in the country through intensifying its supervisory work, educational activities and awareness-raising campaigns.

Inspections, citizens' complaints and consultations

Compared to 2016, 2017 was marked with a 20% increase in the number of inspections conducted by the Office. Swift review was provided to citizens' complaints that have increased by 10% compared to 2016. After five years of intensive work of the Office, positive changes are becoming more evident, especially in public sector and large data controllers in private sector (banks, hotels, pharmacy chains and retail centres, among others). They are better informed about personal data protection issues and try to find systemic solutions to the problems. Consequently, less violations were revealed in public organizations and large businesses. Certain problematic issues remain in medium and small businesses.

In the reporting period the Office studied data processing in public sector, including various ministries, courts, election administration, local self-governments. Lawfulness of processing was checked in more than 70 cases in law enforcement agencies. Cases related to a wide array of processing activities: data transfers, video surveillance, access to databases, identification of individuals, etc.; this also included collection of meta data and video recordings by the law enforcement agencies, where less violations were revealed compared to previous years.

As for private sector, during 2017, the Office of the Inspector studied and reviewed 270 business processes, which included data processing by financial institutions, debt collectors, healthcare institutions and other organizations. Violations in private sector mainly related to disclosing data on the internet, disclosure to third parties, data security, video surveillance at the workplace, audio monitoring, direct marketing, etc.

To prevent further violations, the Office continues to offer guidance to help organizations advance their data protection policies and practices. To this end, more than 4800 consultations have been delivered in

2017 that marked a 25% increase compared to 2016. From this overall number of consultations, up to 900 were delivered to public bodies, more than 1500 − to private organizations and more than 2300 − to individuals.

Educational and awareness-raising activities

Despite the significant progress achieved so far, raising public awareness remains one of the central matters on the agenda. In order to further contribute to the advancement of personal data protection standards in the country, the Office held numerous trainings, seminars and workshops for various public institutions and private organisations and the representatives of the media and civil society.

In January 2018, the Inspector's Office published the English version of the Personal Data Alphabet which is based on the concept of the Alphabet created in Georgian language in 2017. The Alphabet assembles 26 examples of personal data corresponding each letter of the English alphabet and provides brief information about their importance, associated risks and simple tips for their protection in plain language. The Alphabet serves as an awareness-raising and education material for English-speaking audience and can be freely used by any interested party.

At the same time, the Office elaborated tailored recommendations regarding data processing in higher education institutions, a guide for start-ups and is now finalizing the guidelines for healthcare sector. In cooperation with the Council of Europe, the Office was involved in the process of elaborating guidelines regarding the balance between freedom of expression and the right to privacy in media activities.

As the entry into force of the EU General Data Protection Regulation ("**GDPR**") was approaching, Georgian organizations were becoming more interested in the new rules introduced by the regulation, that would affect them as well. Along with providing face-to-face consultations and delivering presentations regarding the GDPR, the Office of the Inspector released a short informational brochure in the Georgian language. The brochure introduces the rules of the regulation and provides necessary information to the relevant audience regarding the compliance requirements in simple language.

Moreover, various communication tools were used to reach the public through TV, website and social media. Information materials regarding data protection were prepared in the languages spoken by the ethnic minorities residing in Georgia as well.

International cooperation

The Inspector's Office actively participated in international data protection cooperation forums and conferences, including the 39th international Conference of Data Protection and Privacy Commissioners (ICDPPC), Conference of European Data Protection Authorities, International Conference on the occasion of the 20th anniversary of the personal data protection law in Poland, etc. The Office also shared experience in various aspects of its work with colleagues from Kyrgyzstan and Belarus as the countries are working to establish a data protection authority. The Office joined the International Working Group on Digital Education and is working with the Ministry of Education and Science of Georgia to include privacy issues in the school curriculum.

LEGISLATIVE AMENDMENTS

Georgia is determined to further enhance data protection legislative framework. In light of the EU data protection reform and modernization of Convention 108, and with the aim to advance data protection standards in the country, the Office is working on legislative amendments. A comprehensive comparative analysis of the EU GDPR and the existing Georgian legislation was conducted, a number of meetings were held with relevant stakeholders and currently the Office is in the process of drafting respective amendments, which will later be passed for relevant legislative procedures.

GERMANY / ALLEMAGNE

Federal Republic of Germany: Major developments in the data protection field since June 2017

1. Beginning of the application of the GDPR and entry into force of the profound reform of national data protection legislation on 25 May 2018

After the EU data reform package had been adopted in 2016 German data protection law had to be brought in line with the new EU requirements. Already 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 which entered into force on 25 May 2018 - i.e. the same day on which the EU General Data Protection Regulation (GDPR) became directly applicable in the entire EU. Furthermore, the German legislature adopted an Act in July 2017 to align the general social data protection law as well as other specific data protection provisions with the requirements of the GDPR; this Act also entered into force on 25 May 2018. Some of the German federal states (“Länder”) already adopted and other German federal states are about to adopt a profound reform of their respective data protection legislation in order to be compliant with the new EU data protection rules.

2. Explaining the new law to controllers, processors and data subjects

It became evident in recent months that there are numerous questions of controllers, processors and data subjects concerning the new EU and national data protection legislation. The Federal Government and the German Data Protection Authorities therefore made a lot of efforts to provide information and to give guidance in order to enable everyone to comply with the new legal framework.

3. Preparation of a comprehensive reform of specific data protection provisions in numerous Federal Acts with a view to the 2016 EU data protection reform package

The reform of German Federal data protection law with a view to the 2016 EU data protection reform package is not yet finished. The Federal government is preparing the alignment of about 150 Federal Acts containing specific data protection provisions in various areas of law.

HUNGARY / HONGRIE

Country report – Hungarian National Authority for Data Protection and Freedom of Information (NAIH)

The year 2017 was clearly spent in the spirit of preparation for the GDPR.

I. Data Protection

In 2017, the management of data protection cases was carried out in accordance with the established procedural order but also in the spirit of the new act on general administration procedure and the preparation of the new General Data Protection Regulation.

Data Protection Cases by type of cases:

- **Submissions requesting information on the enforcement of the GDPR**
  In order to prepare for the application of the new General Data Protection Regulation (GDPR), several data controllers requested the Authority to provide information on the interpretation of the provisions of the GDPR. The amendments of law needed for the implementation of the GDPR in Hungary was being under preparation last year and now, the Authority based its provision of information on data controllers' questions on the text of the Regulation and on the opinions issued by the Article 29 Working Party.

- **Data processing by surveillance cameras:**
  - cameras and camera systems in condominiums
  - camera surveillance at work
  - surveillance cameras in shops
- **Data protection concerns with regard to claims management**
  - prohibition of making environment studies and photos of real property
  - needlessness of examining creditworthiness
  - lack of providing prior information
  - third persons—the prohibition of 'seeing neighbours'
- **Cases of processing photo and scanned copies of identity documents**
- **Health**
  In the field of healthcare data processing, the most important event in 2017 was the launch of the Electronic Health Service Area (EHSA) in practice.

  - According to the agreement concluded by the Authority and the Public Healthcare Supply Centre (hereinafter PHSC), the parties hold consultations on a quarterly basis
  - Copying health records, ensuring the right of access, continues to be the subject of several complaints to the Authority
  - Submissions requesting consultation on health issues showed a variegated picture. There were questions about online appointments, transfer of personal health-history sheet, the mode of operation of surveillance cameras at healthcare provider premises, which obviously differs from other modes of surveillance due to the special personal data being processed at a healthcare institution.
- **The Processing of Children's Data (see NAIH Children's Rights Project)**

Most significant cases in the field of data protection:

- **Administrative procedure on data processing by the former Hungarian Church of Scientology and by the current Association of Scientologists:**

Based upon complaints submitted by citizens NAIH decided to launch an administrative procedure on the data processing carried out by the Hungarian Church of Scientology. During the procedure on site inspection was held at two locations and NAIH seized electronic and paper based data carriers.
In the course of the abovementioned administrative proceedings, the NAIH found that the Church and the Central Organization carry out unlawful data processing activities because of breaching their obligation to provide prior information, the principles of purpose limitation and fairness in data processing, failing to meet data security requirements, and also pursuing data processing without legal basis.
The Authority prohibited further unlawful data processing, and imposed the maximum amount of the data protection fine, HUF 20 million on the Church and the Central Organization each, all together HUF 40 million (~ 125,000 €)
The full English version of the decision can be found on the Authority's website: https://naih.hu/files/Scientology-Decision-final-2018-01-29-.pdf .

- **Data processing at Sziget Festival**

The Authority received several complaints regarding the VOLT Festival and the Sziget Festival, in which the notifiers complained of the organizers' admittance practice of scanning the identity cards of the visitors and not adequately informing the data subjects of the circumstances of data processing, including the purpose and duration of storing copies of the identity cards.

The Authority called on the company to review and modify its admittance system and data processing practices, as well as to prepare its data processing notice and rules to provide adequate information to data subjects. The Authority also called the attention of the data controller to the obligation to comply with the GDPR when reviewing its data processing practice

II. Freedom of Information

2017 was fundamentally geared towards the preparation of the General Data Protection Regulation for both public bodies and the Authority. However, compliance with the new data protection rules did not mean that the other informational right, the freedom of information, was relegated to the background. On the contrary, the Authority paid more attention to the right to access and disseminate data of public interest and data public on grounds of public interest, and to raising awareness of obligations related to the freedom of information.

As in previous years, the Authority focused on the publicity of data on the management and use of public funds and national assets. Public funds and national assets must be managed according to the principles of transparency and the purity of public life. For the realization of the values and goals enshrined in the Fundamental Law, the existence and enforcement of the freedom of information is indispensable.

In 2017, the Authority expanded and developed its practice in the application of the rules of the reimbursement of costs regarding requests for data of public interest. 2017 was the first year in which the relevant regulations were already in force throughout the whole year. The public bodies applied the rules of charging fees in ways that led to infringement of law on several occasions. In each case, the Authority not only tried to consider facts and circumstances relevant to the particular case, but also to provide general guidance to the bodies and persons concerned.

Finally, it should be emphasized that the Authority continued to play an active role in fulfilling the state responsibilities in the prevention of corruption. In addition, the Authority actively participated at international and European forums on freedom of information. These conferences were primarily aimed at fostering closer international cooperation and the harmonization of different national practices.

By way of summary, it can be stated that the current legal environment focuses not only on the fact that a body or person actually fulfils a public service duty as defined by law but also on the fact of disposal and management of national assets. Thus the Fundamental Law and the laws detailing its provisions doubly ensure the transparency of the management of public funds. On the one hand, the Fundamental Law itself

provides for standards of data of public interest and data public on grounds of public interest. Since this is the basis of the Hungarian legal system, it can be stated that the transparency of the management of public funds is ensured at the highest, constitutional level. On the other hand, taking also into account the rules of the National Assets Act and State Assets Act, the provisions of the Privacy Act on the accessibility of data of public interest and data public on grounds of public interest must be applied in this regard.

- **The NAIH's Activities Related to the Prevention of Corruption**
- **Transparency of the Use of National Assets and Public Funds**
- **Rules of the Reimbursement of Costs Regarding Data Requests (in detail)**
  In 2017, the NAIH developed the criteria and methodological principles that were used to examine what constitutes disproportionate use of the workforce when determining the rate of reimbursement. The NAIH considered information such as the number of people working in the public body, the position of the staff participating in fulfilling the data request, and relationship of the position of the staff involved in fulfilling the data request to the ordinary operation of the body, and which basic activity the body could or could not perform due to fulfilling data request. During the investigations, the NAIH asked why the bodies thought the workforce required to fulfil the data request was disproportionate, and that the data the requester wanted to access was of substantial size. The NAIH also took into account the technical conditions at the disposal of the public body (for example, the number of printers and scanners available in the institution, and how long they were used to fulfil the data request). Naturally, it was also necessary to examine whether the data requested was available in the desired format. The NAIH investigation also covered whether the requested data was included the Standard Disclosure List in Annex 1 of the Privacy Act, i.e. data the public body should have already made electronically accessible

III. Legislation

The Amendment of the Privacy Act

Adopted in 2011, the Privacy Act, in our opinion, is an advanced data protection law that has met the requirements of European legal development to a great extent so that the transition to the rules of the GDPR is not going to increase severity. In the fields of data protection regulation remaining under national legislative competences, it is advisable to develop a data protection regulatory environment by the amendment of the Privacy Act that approximates the GDPR in terms of its conceptual framework, principles, and legal institutions, since it is beneficial to both data subjects and data controllers if the general rules of data protection provide for a more unified and transparent system of legal requirements. Compliance with the new data protection rules is not only a priority for the NAIH, but data controllers and data processors also need to start reviewing their data processing practices in a time.

Under the agreement between the Ministry of Justice and the NAIH, the NAIH had the opportunity to take part in the preparatory work for the Amendment of the Privacy Act from the outset, January 2017. By way of official meetings and delivery of comments, there has been a regular direct working relationship between the two bodies at administrator level to develop the concrete content of the rules and to clarify the issues.

In identifying legislative tasks, the NAIH took the view that there is no likelihood of a need arising to modify the parts concerning the freedom of information, since the relevant EU acts only govern the processing of personal data and the flow of personal data. In order to comply with the EU obligation, it seemed therefore sufficient and appropriate to amend only the provisions concerning the same subject in the Privacy Act.

The independent status of the NAIH is based on the Fundamental Law, and it can be stated on the basis of the examination of the Hungarian laws on its powers, management, and organization that they are in accordance with the EU legislation prescribing the independence of the supervisory

authorities of the Member States and its specific conditions, so we argued that the current provisions of the Privacy Act are also suitable for the enforcement of EU rules.

In terms of substantive rules, we represented the expectation that there should be no stepping down from the high level of protection already provided by the Privacy Act.

In shaping the new procedural rules for the Privacy Act, we kept in mind that the NAIH should be able to exercise its obligations under EU law, and to exercise its new powers in accordance with constitutional requirements, and that the new procedural order can be integrated seamlessly into (the now more direct) international cooperation between the supervisory authorities of the Member States. Another factor to be taken into account is that Act CL of 2016 on General Public Administration Procedures, effective as of 1 January 2018, applies to several procedures falling within the competence of the NAIH. Thus, concord has to be achieved with these rules likewise.

Drafted in close cooperation between the Ministry of Justice and the NAIH, the bill underwent social and administrative consultation until September 2017; all competent organizations had delivered their comments on the draft. At the time of writing this report, the bill was not put on the agenda of Parliament.

The review of sectoral laws in accordance with the GDPR and the amendment of the Privacy Act began in 2018, and this will therefore be discussed next year's report.

IV. Projects

- **International projects:**

  - **Macedonian project (within the tender called „Support to access to right on protection of personal data in Macedonia (EuropeAid/135668/IH/SER/MK")**

    In the framework of the tender called „Support to access to right on protection of personal data in Macedonia", in which the NAIH is a consortium partner, and which is financed by EUROPAID, study visits in the Republic of Macedonia continued in 2017. The three topics the NAIH experts focused on were: international cooperation in data protection, harmonization of the two informational laws and data protection cases of the courts, prosecution and the ombudsman's data processing. As part of the project, staff members of the Macedonian Data Protection Authority visited the NAIH in Budapest, and got acquainted with its internal operation and procedures, visited Magyar Telekom Nyrt, and consulted with data protection officer of the company.

  - **The STAR Project**s

    STAR I: In November 2017, the start of our new EU data protection project—STAR (Support Training Activities on the Data Protection Reform)—began with the kick-off meeting in Budapest. The 24-month project is co-funded by the European Union, and alongside NAIH, partners are the Vrije Universiteit (VUB) in Brussels and the British Trilateral Research Ltd (TRI), and the objective is the compilation and testing of training material on the GDPR for data protection authorities and data protection officers. For further details about the project, visit https://projectstareu.wordpress.com/.

    STAR II is addressed to 40+ EU DPAs and millions of EU small and medium enterprises (SMEs). It will deliver tangible and long-term results to SMEs, directly assisting them in compliance with the GDPR (by hotline and guidance material) and – indirectly – to DPAs, to assist in their awareness-raising mission.

- **A Small Key: The Continuation of the NAIH Children's Rights Project**

The Hungarian DPA has laid particular emphasis on the protection of the personal data of children; this was why we published our volume of studies entitled Key to the World of the Net! on the Internet habits of children between 10 and 16 (a new edition of which came out in 2016, updated and supplemented with current topics); we launched our awareness campaign with Tamás Vastag's song in 2014; and we joined the ARCADES project of the European Union whereby reference books on data protection were published for teachers (in Hungarian, too).

The aim was always the same: to help children and youths—directly and by way of assistance from adults responsible for their upbringing—live consciously in the world of the Internet, not only be smart but also knowledgeable at using these devices, and also to take responsibility for others in virtual reality, as well.

In 2017, the NAIH has thus focused on children under 10. This study volume seeks to map those sources of danger that might infringe on the privacy kindergarten and school children, the protection of their personal data, and thereby damage their future healthy development. Our aim is certainly not to deter; rather, it is to call attention to digital-space phenomena that may affect the youngest age groups now and in the future.

V. Control of Classified Data—Classified-data Cases

So-called classified-data cases make up a heterogeneous part of the Authority's duty portfolio. The cases belonging here may be related to both the protection of personal data and access to public data. Neither can they be considered as uniform from the point of view of procedural law, because, from among the proceedings under the Privacy Act, not only may administrative proceedings for the control of classified data touch classified data but also investigation proceedings, administrative proceedings for data protection, and data protection audits; moreover delivering opinion on draft legislation may concern basic information rights related to classified information. The Authority may, in the case of national security data, examine whether its classification is lawful, or whether its classification violates the right to the protection of personal data or to the access and disclosure of data of public interest. In the case of foreign classified data, the review of its classification falls outside the competence of the Authority.

ICELAND / ISLANDE

Information on Major Developments in the Data Protection Field
June 2017 – June 2018

The Icelandic Data Protection Authority
At this time, 12 people work at the Icelandic Data Protection Authority, including eight lawyers, an information security expert, an archivist, an office manager and the Data Protection Commissioner, Ms Helga Þórisdóttir. The chair of the DPA‘s board of directors is Ms Björg Thorarensen.

On 1 January 2018, the DPA‘s annual budget was increased by approximately 80%, i.e. from 114,2 million ISK (Icelandic kronas) to 205,8 million ISK, due to heavy workload at the authority and the forthcoming General Data Protection Regulation.

In addition to this, the DPA‘s funds will be gradually increased every year for the next four years, according to a new government budgetary plan. This will allow the DPA to hire an estimated 10-15 more people in this period.

General Data Protection Regulation (GDPR)
A Joint Committee Decision incorporating the GDPR into the EEA agreement is expected to be adopted by the EEA Joint Committee on 6 July 2018 and enter into force in Iceland, as well as the other EEA EFTA states, in mid-July 2018.

Furthermore, the Icelandic parliament, Alþingi, is currently discussing a new government bill of law on a new Data Protection Act, based on the GDPR. The bill is expected to be passed this week.

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 2018
The DPA participated in UT-messan, one of the largest IT events in Iceland. The event was twofold – a conference for the IT industry and a big exhibition. One of ten tracks at the conference focused on Data Protection and was organised in collaboration with the DPA. One of four keynote speakers at the conference talked about data protection (Marc Rotenberg, from the Electronic Privacy Information Center („EPIC“)), and four other speakers gave speeches at the Data Protection track of the conference, including the Norwegian Data Protection Commissioner, Bjørn Erik Thon.

Another event organised for the Data Protection Day was an open seminar, held by Orator, the law students‘ society at the University of Iceland. The chair of the DPA‘s board of directors, Ms Björg Thorarensen, who is also a law professor at the university, gave a general introduction of the GDPR at the seminar.

Data Protection seminar for the Health Sector
On 12 January 2018, the DPA held a seminar on the GDPR and data protection in general, specifically designed for the Health Sector, at the National University Hospital of Iceland. The event was open to all health professionals in Iceland and was attended by approximately 200 people. The event was also streamed online and viewed by several hundred people.

Data Protection seminar for the Education Sector
On 9 November 2017, the DPA held a seminar on the GDPR and data protection in general, specifically designed for educators and others working with personal data in the school system (from kindergarten to universities). The event was advertised and open to the public. It was also streamed online, and the recordings were later published at the DPA‘s website.

Data Protection seminars for the Public Sector
In 2017, the DPA held a total of three seminars on data protection and the GDPR, specifically designed for the public sector (one seminar for ministry experts and two seminars for other officials tasked with GDPR implementation within their organisations). Only 4-5 seats were available for each organisation/ministry and they were reserved for those members of staff responsible for implementing the GDPR in each organisation/ministry.

Data Protection seminar for the Court System
In May 2018, the DPA held a seminar on the GDPR, and data protection in general, specifically designed for the court system. The Icelandic courts were closed for the day, and all judges and other staff were expected to attend the seminar. The publishing of personal data on the Icelandic courts' websites, where some of the courts' rulings are published, has been much discussed in Icelandic society lately and the DPA is working with the courts on reviewing current practices in this regard.

Media Coverage
Data protection has been an extremely popular subject with the Icelandic media over the last two years. The DPA's rulings are frequently reported and the Data Protection Commissioner has been interviewed and asked to comment on multiple data protection-related subjects in newspapers, online media, radio and television.

Other events
The DPA has given lectures and presentations on GDPR and other data protection-related matters on many occasions in the past year.

Further awareness-raising activities
The Icelandic DPA recently applied for and received a grant from the European Union's Rights, Equality and Citizenship work programme. The grant will support the DPA's awareness raising activities aimed at the general public, including children, and businesses, in particular small and medium size enterprises.

Statistical Data
According to statistical data, during 2017 the DPA received a total of 1.911 new cases, compared to 1.865 cases in 2016. In the first four months of 2018, the DPA has seen a 27% increase in the number of cases, compared to the year before. At this time, there are 708 open cases at the DPA.

IRELAND / IRLANDE

Report from Ireland on Major Developments (June 2018)

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 Protection Act 2018
The Data Protection Act 2018 was enacted in May 2018. The key purposes of the Act are as follows:

- to give further effect to the General Data Protection Regulation in the areas in which Member State flexibility is permitted;
- to transpose the law enforcement Directive into national law;
- to establish the Data Protection Commission as the State's data protection authority with the means to supervise and enforce the protection standards enshrined in the GDPR and Directive in an efficient and effective manner, and
- to enact consequential amendments to various Acts that contain references to the Data Protection Acts 1988 and 2003.

Establishment of Data Protection Commission
The Data Protection Act 2018 provides for the replacement of the Data Protection Commissioner with the Data Protection Commission with up to three commissioners. The Commission was established on 25 May. While there are no specific plans at present to increase the number of Commissioners, significant levels of additional financial and staffing resources have been allocated to the Data Protection Commissioner in recent years in order to prepare for the expected workload increases following entry into force of the GDPR and the Data Protection Act. The budget has been increased from just under €2m in 2014 to about €11.7m in 2018. Staff resources have more than trebled from 30 in 2013 to almost 100 at present. It is planned that additional staff will be recruited in 2018 bringing the total number to about 140.

Data Protection Commissioner Annual Report 2017
The 2017 Annual Report of the Data Protection Commissioner was published in February 2017. The Report highlights key developments and activities of the Office in 2017, together with priorities for the coming years. The Report is available at:
https://www.dataprotection.ie/docs/EN/27-02-2018-Commissioner-publishes-Annual-Report-2017/m/1697.htm

Data Summit 2018
The Department of the Taoiseach (Prime Minister) is currently planning the Data Summit 2018, a follow up to last year's very successful event, which involved many internationally recognised speakers and attracted a large national and international audience from a range of disciplines.

The 2018 event, scheduled to take place on 19 September 2018, seeks to highlight many of the important initiatives and developments that are originating from the European Union, such as the implications of the General Data Protection Regulation and the initiatives relating to Artificial Intelligence. The event will be a key element of Ireland's work to demonstrate real leadership and drive the debate in the development of policy and best practice around the area of data and data privacy.

Proposed National Digital Strategy
The Action Plan for Jobs 2018 commits to the development of a framework for a high level National Digital Strategy. The purpose of the Strategy is to provide a coherent vision across sectoral policies, which relate to digital matters. The Strategy will enable Ireland to maximise the economic and societal benefits that arise from ongoing digitalisation and its transformative effects.

An Interdepartmental Group has recently been established to support the development of the new National Digital Strategy. The Strategy will provide for a national narrative to understand the impacts of digital technology on Ireland and help all groups to assess how they can make the most of continuous digital transformation.

ISRAEL

Country Report for the State of Israel

1. In Israel, according to the Basic Law: Human Dignity and Liberty, 1992, the right to privacy is a fundamental basic human right that receives constitutional protection – the right must be respected by every government authority, unless by means of a Law, or according to an explicit authorization therein, which serves an appropriate purpose, and to an extent that does not exceed what is required in order to fulfil the purpose of the law. In addition, the principle of structured balancing between fundamental rights and interests, and the principle of proportionality with regards to the right to privacy are enshrined in Israeli Administrative Law and in Judgments of the Israeli Supreme Court. Therefore, these principles are a significant part of our legal system and are rooted in our legal framework.

2. The Israeli Privacy Protection Law, which was enacted in 1981 and was amended since then several times, is one of the first privacy laws in the world. The Law provides for the protection of several aspects of the right to privacy, amongst them data protection, and applies on both public and private sectors.

3. The Privacy Protection Authority enforces the provisions of the Privacy Protection Law with regards to data protection. According to the Law, The Registrar of Databases – acting within the organizational framework of the Privacy Protection Authority – has the power to demand information, launch uncoordinated onsite inspections and conduct criminal investigations for violating provisions which their violation constitutes a criminal offence.

4. Israel was recognized in 2011 by the EU as providing an adequate level of protection for personal data according to Directive 95/46/EC. In addition, the Privacy Protection Authority cooperates with DPA's around the world through its membership in a variety of international organizations and is a member of the SPDE, the Berlin Group and the ICDPPP and the GPEN Committee.

5. Following the request of the Secretariat regarding major developments in the data protection field in the last year, we would like to report about 3 such developments in our legal and regulatory framework:
New Privacy Protection Bill regarding Enforcement Powers.

6. As aforementioned, The Registrar of Databases – acting within the organizational framework of the Privacy Protection Authority – is granted with powers in order to enforce the provisions of the law regarding data protection.

The purpose of the new bill is to improve these supervision and enforcement capabilities and supervisory mechanisms of the authority, in order to enable it to cope in a more effective manner with the updated risks threatening the right to privacy and personal data. The bill proposes, *inter alia*, to extend the authority given to the regulator, and to grant him the authority to conduct administrative inquiries into administrative violations and criminal enforcement. An important tool that the bill proposes to make available to the regulator is the authority to impose financial sanctions. The expansion of the "toolbox" available to the regulator by way of establishing an alternative mechanism to the criminal procedure will enable a quick, efficient and proportionate response to violations of the law. This sanction will be imposed in a gradual manner that is appropriate to the types of violations, their severity and the circumstances in which they were made.

The new Bill had passed the first reading in March 2018.

New Data Security Regulations

7. **New Data Security Regulations** that came into effect on May 18th- the Privacy Law obligates controllers to secure data with reasonable means. The new regulations provide a robust methodology to manage date security in organizations. The regulations are based on common acceptable standards and make them mandatory, contrary to most other jurisdictions in which, as far as we know, those standards are not legally binding.

The regulations include a variety of provisions with regards to breach notification, accountability obligations, and keeping records of processes; log-ins, securing communications, encryption obligations, access controls, physical security and more.

Please find attached to the report a brief of the regulations.

Data Protection Regulations.pdf

Strategic change in the Privacy Protection Authority

8. In order to advance and improve the Israeli Privacy Protection Authority's capabilities in coping with future challenges to data protection, and in order to strengthen the Privacy Protection Authority (hereinafter: the PPA) and enable it to fulfill its' tasks in an environment that is exposed to far-reaching and ongoing developments in the digital space, the authority went through a significant strategic change that includes re-organization of its structure and modifying and re-prioritizing its aims.

9. In order to implement the changes the PPA's budget and team was increased significantly.

10. The PPA was able to convince the government that strengthening data protection will increase the trust in the digital economy, which is fundamental for the Israeli economy, given the prominent role of high tech in Israel, a phenomenon because of which Israel is known as the "start - up nation".

11. The government increased the PPA's budget by more than 100% (the initial budget grew from 8 million NIS to 16.5 million NIS) and its staff increased by 25%. The PPA's staff includes lawyers, computer engineers, and data security professionals.

12. The budget has increased dramatically although the PPA initiated another change – until recently, database owners needed to pay an annual fee. The PPA wanted to remove regulatory burdens and the annual fees were cancelled.

13. As aforementioned, the PPA is empowered to conduct criminal and administrative investigations. The PPA may issue fines and terminate the activities of databases that infringe the Privacy Protection Act. The PPA conducts its investigations using a "top of the line" forensic laboratory which is operated by its professionals.

14. Audits - A major development in the PPA's enforcement activities is the fact that the PPA intends to use its budget to investigate and supervise more sectors and companies by deploying a new audit mechanism. This new mechanism will enable the PPA to reach out to a wide range of sectors and organizations, to receive information, examine practices and their compliance with the law. The findings will enable the PPA to instruct organizations and guide them with regards to data protection and this is a meaningful tool to engage in a dialog with organizations and for "soft regulation".

15. Guidelines and standardization as an alternative for "Case by Case" advice and guidance – the PPA realized that known standards and guidelines will assist organizations to increase data protection and avoid infringements and unnecessary enforcement actions. During the past year and a half, the PPA issued guidelines and standards, reflecting its interpretation of the Privacy Protection Law, which were drafted after public consultations. The guidelines were made public in the PPA's website, and enjoyed wide media coverage.

16. The Department for Strategic Alliances - In order to engage with all the stake holders in the digital economy, the PPA established the Department for Strategic Alliances. The new department was established in order to create and promote a meaningful public debate on privacy, and engage the public, in order to establish privacy protection awareness and actions. The department's responsibilities include: Communications, PR, New-media; Policy Delivery; Government and Parliament relations; Training and Education; Conferences organization & participation;

17. Since its initiation the department has accomplished the following: Creating a dominant presence in the media with numerous written, radio and television appearances; creating a social media presence with an active Facebook account; establishing a forum for privacy awareness & training in the Israeli public sector which currently includes 140 members, from both legal and tech background and positions, meeting 4 times a year and receiving monthly updates. The establishment of this forum is another step towards introducing the requirement to appoint privacy champions in public bodies; a similar forum for the private sector will be developed in the future in order to engage in a dialogue with the industry and civil society; sending a monthly newsletter including updates of activities in both enforcement, guidelines and events to a list of approximately 3,000 followers from the professional community; writing Q&As for the PPA's guidelines and working on a guide to the new Israeli Security Regulations in order to make the regulatory regime more accessible to the public; re-building the PPA's website with an approachable concept and updated content; the new website is very accessible and is aimed to different communities (an English version of the new website will be launched in the near future as well), re-branding the PPA (previously LILTA) with a new name and logo dedicated to privacy protection;

18. Establishment of Department for Innovation and Policy Development – the new department is tasked with the mission of identifying innovative trends in the field of technology, business and social privacy, conducting research and initiating innovative regulatory solutions to data protection in the sophisticated and dynamic digital economy. In addition, the department will consult the Head of the PPA in the process of determining the PPA's policy and strategic planning.

19. All of the abovementioned developments were promoted based on the importance given to the constitutional right to privacy, and according to the understanding that in light of the rapid technological changes, and given the prominent role that data protection plays in building trust in the digital economy – the challenges to privacy are increasing and therefore privacy protection must be increased accordingly.

JAPAN / JAPON

Major developments in the data protection field in Japan

1. Strengthening and expanding the structure of the PPC

The Personal Information Protection Commission (PPC) is composed of the chairperson, eight commission members and four specialist commissioners. From last autumn, the number of specialist commissioners in charge of investigation of international projects, etc. has been increased from one to four to strengthen the organizational structure for conducting surveys of foreign systems and cooperation with foreign related organizations. In particular, one of the four specialist commissioners is specialized for introducing the activities of PPC to academic experts, exchanging views, investigations, etc. The other three expert commissioners are working with data protection authorities and practitioners. Therefore, the PPC has been focusing on cooperating with a wide range of academic experts, data protection authorities and practitioners.

In addition, the secretariat of the PPC increased the number of lawyers and IT experts last fiscal year. The secretariat is focusing on expanding the system for operations which require specialized knowledge and currently secures more than 130 staff members including experts in various fields such as lawyers, accountants, IT experts.

2. Information and edification activities

Since September 2015 when the amended Act on the Protection of Personal Information (APPI) was promulgated, the PPC has been holding a number of seminars targeting business operators continuously aiming for disseminating the contents of the amended APPI. From July 1, 2017 to the end of May 2018, the PPC held 100 seminars dispatched lecturers to briefing sessions and got 7,300 participants. The PPC has also held briefings at international conferences to disseminate the Act on the Protection of Personal Information.

In reaction to recent various privacy concerns raised over SNS, the PPC gave site managers and users an attention respectively concerning collection of the information through third party.

On May 30 this year, the PPC celebrated the 1st anniversary of the application of the amended APPI. Therefore the PPC Japan, as a member of APPA, decided to set "Privacy Awareness Week" from May 21st to May 31st, including the one year celebration date of full implementation of the amended APPI. The PPC Japan backs up and dispatches speakers to the symposium which is held during this period.

3. International activities

(1) Participation in International Cooperation Frameworks

The PPC was approved as an accredited member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) at the 39th conference of ICDPPC in September 2017.

At the conference, Dr. Horibe, the Chairman of the PPC, expressed gratitude for being approved as an accredited member of the ICDPPC, and introduced the legal system on the personal information protection in Japan and the PPC's activities at the conference. In addition, he observed "Through those activities, I would like to further contribute to connecting the East and the West."

Furthermore, the PPC held a workshop on CBPR as the side event of the conference. The workshop was the most flourishing one among the events in the same time zone.

(2) Promotion of APEC/CBPR System and certification of a new business operator

The APEC/CBPR system, which is a scheme among APEC member economies to certify a business operator's compliance with the APEC Privacy Framework, is an effective international standard to assess a business operator's standard of personal information protection. With this recognition, the PPC has actively promoted the CBPR system. From July 1, 2017 to the end of May 2018, the PPC held 9 seminars at international conferences and got 910 participants.

Obtaining the CBPR certification brings benefits for the Japanese companies expanding their business internationally, therefore the PPC has been briefing the CBPR system in various seminars in order to disseminate the CBPR system. During the above mentioned period, the PPC held 60 seminars and got 5,300 participants.

In this May, JIPDEC, the accountability agent in Japan, certified a new business operator as the CBPR certified organization, as a result, the certified organizations became two.

(3) Dialogues on the mutual and smooth personal data between Japan and EU

PPC has had dialogues with European Commission many times since last year before last to enhance mutual and smooth personal data transfer between Japan and the EU for the mutual certification which mutually recognizes to have adequate level of data protection. Both commissioners held a dialogue on May 31 and agreed to finalize both procedures as soon as possible and these procedures are in the finalization phase.

This framework of the mutual certification between Japan and the EU is an epoch-making effort, and it can be a global model when the effort fruits.

PPC continues to have dialogues energetically to finalize the work.

LIECHTENSTEIN

La révision de la loi nationale portant sur la protection des données a été préparée par le gouvernement et sera traité par le parlement lors d'une première lecture au début de mai et lors d'une deuxième lecture en automne. L'entrée en vigueur est prévue pour la fin de l'année, selon toutes prévisions en novembre. Il s'agit d'un projet de loi à grande échelle qui comprend au delà de la loi sur la protection des données aussi des dispositions dans d'autres lois nationales portant sur la protection des données.

Il est également prévu de soumettre au parlement en mai une loi transitoire qui permettra à l'autorité de protection des données à exercer les compétences prévu par la RGPD (à l'exception des sanctions) à partir de l'application de la RGDP au Liechtenstein (probablement en début juillet).

MAURITIUS / MAURICE

In 2017, the Data Protection Act 2004 was replaced by a new and more appropriate legislation known as the Data Protection Act 2017 which came into force on 15 January 2018 in Mauritius.

The new DPA aims at strengthening the control and personal autonomy of data subjects over their personal data, thereby contributing to respect for their human rights and fundamental freedoms, in particular their right to privacy, in line with current relevant international standards, in particular the European Union's Regulation on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, commonly known as the General Data Protection Regulation (GDPR).

MEXICO / MEXIQUE

MEXICO'S MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD

The purpose of this document is to report on the regulatory advances on personal data protection that took place in Mexico from June 2017 to May 2018.

1. Standards for personal data protection for Ibero-american States (This is a collective effort of the members of the Ibero-American Data Protection Network)

The Ibero-American Standards constitute a set of guidelines that may contribute to the issuance of regulatory initiatives for the protection of personal data in the Ibero-American region, which encompasses those countries that do not have these regulations yet; or, if it were the case, they may serve as reference for the modernization and updating of existing legislation.

The following are some of the objectives of the Ibero-American Standards:

- To guarantee the effective exercise and guardianship of the right to the protection of personal data of any person in the Ibero-American States, by establishing common rules that ensure due treatment of their personal data.
- To make the flow of personal data between Ibero-American States and beyond their borders easier, in order to contribute to the economic and social growth of the region.
- To foster international cooperation amongst controlling authorities of the Ibero-American States, with other non-regional controlling authorities, and with international authorities and agencies in this field.
- To establish a set of common principles and rights for the protection of personal data which could be adopted by the Ibero-American States and develop their national legislation thereon, with the goal of having homogenous rules in the region.
- To raise the level of protection of natural persons regarding the processing of their personal data, as well as between the Ibero-American States.

Available at:
http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf

2. Administrative provisions of a general nature for the development, presentation and evaluation of data protection impact assessment

The objective of the administrative provisions is to establish the general framework applicable in the development, presentation and evaluation of data protection impact assessment. It is a document through which any data controller who intends to put into operation or modify public policies, programs, systems or computer platforms, electronic applications or any other technology that involves the intensive or relevant treatment of personal data, assesses the real impacts to the right to the protection of personal data in order to identify and mitigate possible risks related to the principles, duties, rights and other obligations provided for in the relevant legislation on this matter.

These impact assessments seek to detect, prevent and minimize risks that could affect data subjects and, even more, prevent the impact on economic costs with respect to those treatments that, from their origin, are not aligned with the corresponding regulations.

Available at: http://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018

3. General criteria for the implementation of compensatory measures in the public sector of federal, state and municipal order

Its objective is to establish the parameters through which any authority, dependency, entity, organ or agency of the Executive, Legislative and Judicial Branches, autonomous constitutional bodies, administrative tribunals, trusts and public funds, of federal, state and municipal order, as well as political parties, may implement compensatory measures.

The compensatory measures are alternative mechanisms to inform data subjects of the simplified privacy notice, through its dissemination through mass media or other wide-ranging mechanisms when it is impossible to publicize the privacy notice to the data subject directly or when it implies disproportionate efforts.

Available at: http://www.dof.gob.mx/nota_detalle.php?codigo=5511114&fecha=23/01/2018

4. General Guidelines for the Protection of Personal Data for the Public Sector

Its objective is to facilitate and make more understandable and simple the knowledge and enforceability of the right to the protection of personal data in the federal public sector, as well as to avoid the existence of innumerable ordinances that could affect the effective fulfillment of the General Law on Protection of Personal Data Held by Obligated Parties, or make inaccessible the right for any person.

Available at: http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

5. Agreement by which it is approved to reform articles 2, fractions II, III, V, VI, IX, X, XII, XIII, XIV, XV and XVI; 4; 6; 9, sections II, sections A and B and XII; 11, fraction III; 12, section A, section III and section C, section II and 13 of the General Guidelines for the National Institute of Transparency, Access to Information and Protection of Personal Data to exercise the faculty of attraction.

The purpose of the reform is to recognize the elements that the Institute must assess in the exercise of its power of attraction over those review appeals that are, in principle, the responsibility of local supervisory authorities, but due to its interest and transcendence those review appeals must be known and resolved when approved by the majority of INAI's Commissioners.

Some elements that the Institute must take into consideration to exercise its faculty of attraction are: the purpose of the processing of personal data; the number and type of data subjects involved in the processing of personal data carried out by the data controller; the sensitivity of the personal data; the possible consequences that would derive from an undue or indiscriminate treatment of personal data, as well as the relevance of the treatment of personal data, in attention to the social or economic impact of such treatment and the public interest to know about the review appeals, as well as the review resources on personal data protection.

Available at: http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.11.pdf

6. Guidelines that establish the parameters, modalities and procedures for the portability of personal data

The purpose of these Guidelines is to establish the parameters to be considered in order to determine the cases in which the existence of a structured and commonly used format containing personal data is considered, as well as the technical standards, modalities and procedures for the transmission of such personal data to guarantee the portability of the personal data referred to in the General Law on Protection of Personal Data Held by Obligated Parties or in the local legislations.

This applies to the obliged parties of the General Law that have systems that allow generating structured and commonly used formats to provide data subjects with a copy of their personal data so that they can be reused and / or exploited or for the transmission of this data, with the objective of making effective the

portability of personal data established in article 57 of the General Law or in the corresponding articles of the local laws.

Available at: http://www.dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018

7. Accession to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and to its additional Protocol (CETS No. 181)

The Committee of Ministers, in its 1302nd bis meeting that took place in 13 December 2017, agreed to the request of Mexico to be invited to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and to its additional Protocol (CETS No. 181).

The President of Mexico, Enrique Peña Nieto, asked the Senate of the Republic to consent to the accession to Convention 108 and its Additional Protocol.

On April 26th, 2018, the Senate approved the accession of Mexico to these international instruments.

Available at: http://www.senado.gob.mx/sgsp/gaceta/63/3/2018-04-26-1/assets/documentos/Dic_REE_Consejo_Europa_proteccion_datos.pdf

8. Guide for the Treatment of Biometric Data

Its objective is to guide those data controllers and data processors of both, public and private sectors, to handle biometric data in accordance with the principles, duties and obligations set forth in the General Law on Protection of Personal Data Held by Obligated Parties and in the Federal Law on Protection of Personal Data Held by Private Parties.

Available at:
http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

MOLDOVA

Major developments in the data protection field of the Republic of Moldova

The necessity to ensure an adequate level of personal data protection, respect for the rights of data subjects, including the right to privacy - equivalent to that existing in the European Union (EU), remains a priority, as reflected in the main documents on the European integration process of the Republic of Moldova (RM).

1. **Harmonization of the national legal framework in the field of personal data protection to the EU law, with a particular emphasis on Regulation (EU) 2016/679 of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and Council.**

In the context of NCPDP co-operation with the Council of Europe, on November 8, 2017 were presented the opinions of the Council of Europe experts on legislative amendments proposed by NCPDP to the draft law on the National Center for Personal Data Protection and draft law on amendment and supplement of some legislative acts, in particular Law no.133 of 8 July 2011 on the personal data protection.

It has been found that the draft laws do not contradict the provisions of Convention 108 and its updated version. It was also an opportunity to present to the public the draft laws drafted by CNPDCP and to have discussions with civil society and the private sector.

On October 2, 2017, the Twinning project "Strengthening the Capacity of the National Center for Personal Data Protection in the Republic of Moldova" started. The project is funded by the European Union. It should be mentioned that the draft laws mentioned above were subject to analysis, debates, proposals and discussions at several meetings with experts from EU countries (Germany, Latvia, Estonia, Hungary), in the framework of ongoing Twinning project.

Currently, both draft laws have been finalized and submitted to the Government for approval.

Also, we mention that NCPDP representatives attended the 3rd Association Committee on the Association Agreement, which took place in Chisinau, on October 19, 2017, presenting to the representatives of the EU Delegation in the Republic of Moldova and the European External Action Service the actions undertaken by NCPDP during the year 2017.

2. **Adopting efficient measures to strengthen the statute, structure, staff and financial arrangements of the National Centre for Personal Data Protection**.

On August 19, 2017, in the Official Journal of the European Union was published the new Association Agenda, identifying the priority areas for implementing the provisions of the Association Agreement Republic of Moldova –European Union for 2017-2019.

Thus, point 2, subpoint. 2.4. "Cooperation in the area of Freedom, Security and Justice", in the compartment related to data protection includes the mention of the continued collaboration of the parties in order to strengthen the capacities of the National Center for Personal Data Protection.

The current activity of the Center is regulated by Law no. 133 of 08.07.2011 regarding the protection of personal data and Law no. 182 of 10.07.2008 regarding the approval of the Regulation of the National Center for the Personal Data Protection, the structure, the limit of the staff and the way of Center's financing.

Regarding the increase of the staff of the Center up to 45 units it is mentioned that the evaluation of the increase or necessity of the increase was in relation to the activity of the Center for the years 2013-2015 and the fact that Regulation (EU) 2016/679 and Directive (EU) 2016/680 have not been taken into

account, which completely changed all the rules of personal data processing, including the current normative framework by which the Center was invested with new competences because the evaluation stage did not exist and the number and complexity of the examined cases increased in each year in arithmetic progression.

At the same time, we communicate that the Parliament of the Republic of Moldova by the Law on Electronic Communications, no. 241-XVI of November 15, 2007, republished in the Official Gazette of November 17, 2017, **assigned the Center on the basis of art. 71 with new competencies, namely the verification of appropriate technical and organizational measures in order to protect the security of electronic communications services providers.**

In the same context, with the entry into force on February 23, 2018 of the Law on the prevention and combating of money laundering and financing terrorism, the **Center was empowered to carry out the control of compliance in the part dealing with the processing of personal data by the authorities specialized in the prevention and combating of terrorism, including the Anti-Money Laundering Service,** being transposed the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing**.**

Another law that brought new tasks to the Center is Law no. 120 of 21 September 2017 on the prevention and combating of terrorism. **Counter-terrorism prevention and counter-terrorism activities will be specifically exercised by the Security and Intelligence Service, which processes a very large volume of personal data. Regarding the control of the conformity of the personal data processing the Parliament assigned the Center.**

Under these conditions, the new attributions already given to the Center through the above-mentioned normative acts, as well as by other normative acts, fundamentally change the scope of the investigation activities and conformity assurence of the processing of personal data, taking into account the fact that the authorities subjects to control, process a huge amount of personal data they are assigned to, including state secret, commercial, banking, etc.

Thus, at present, the functioning of the Center no longer meets the challenges and tasks it has, including in terms of payroll and the number of employees. At this point, the number of employees is to be revised by a significant increase.

Taking into account the provisions of Regulation (EU) 2016/679 and Directive (EU) 2016/680, all staff of the European Data Protection Authorities have been increased.

In response to these challenges, NCPDP has drafted a draft law on the National Center for Personal Data Protection, which is currently submitted to Government for approval.

3. **Assessing the compliance of the Moldovan data protection legislation with the new EU legal framework within the Twinning project "Strengthening the Capacity of the National Center for Personal Data Protection", including implementation aspects.**

In parallel with organisational and legal developments, NCPDP benefits from Twinning project in order to strengthen its institutional capacity. This project is funded by the European Union and it is implemented in cooperation with public authorities from Germany and Latvia. The program has started on the 2nd of October 2017 and will be run for two years (October 2017 - October 2019). It pursues 3 key objectives:

1 - Harmonization of the national personal data protection legal framework with that of the European Union.
2 - Strengthening the NCPDP capacities for the effective application of personal data protection national legislation.

3 – Raising public awareness on personal data protection principles.
This external assistance project is intended to support both the efforts in harmonising national legislation and in familiarising the NCPDP staff with the good practices at European level.
Until now, within the Twininng project have been implemented the following actions:

- The table of concordance between the national data protection legislation and GDPR and the table of concordance between the national data protection legislation and the EU Directive 2016/680 has been drawn up.

- trainings with EU experts for NCPDP staff on the applicability of European legislation (GDPR 2016/679 and Directive 2016/680)were organized;

- an Impact Assessment of the EU Regulation(GDPR) for Private Companies in Republic of Moldova was developed and published on the NCPDP site in two languages (Romanian and English).

- A series of working meetings was organized by EU experts, with the participation of NCPDP employees, the business environment, representatives of the law enforcement where were presented the findings, analyzes, conclusions and implementation of the European law in the national legislation.

- The draft law on the protection of personal data and the draft Law on the National Center for Personal Data Protection was discussed, debated, analyzed in accordace with Regulation (EU) 2016/679 and Directive (EU) 2016/680 including within working sessions organized by experts with the representatives of prosecution, police, National Center of Anti-Corruption, customs services, penitentiary institutions etc.

Obtaining observer status

Additionally, we communicate that, after a series of meetings and the follow-up of considerable work, at the plenary meeting of 3-4 October 2017, the Republic of Moldova, has been accepted as an observer member of the Data Protection Working Group of ARTICLE 29 of the European Union. The Republic of Moldova attended the first meeting on 27-29 November 2017. Starting 2018 the Working Group of ARTICLE 29 has changed its name in European Data Protection Board (EDPB).

The acceptance of the Republic of Moldova as an observer member of the European Data Protection Board is a premiere and an achievement in the eastern area, or currently, the Republic of Moldova is the only state that holds this status in the European Data Protection Board, an achievement that will strengthen the relations between the Republic of Moldova and the European Union, both under economical and political aspect.

It is worth mentioning that the Republic of Moldova has all the rights (the right to comment, to participate in the sessions, the right to be informed about ongoing activities and to participate in the debates), with the exception of the right to vote.

Through this international forum the Republic of Moldova will promote the interests of the state in order to adjust and comply with the European Union standards in the field of personal data protection.

At the same time it is stated that obtaining observer status in the European Data Protection Board is an important step towards the recognition of the Republic of Moldova as a third country that ensures a level of protection of personal data equivalent with the European Union.

In order to file an application for recognition as a third country providing an equivalent level of protection of personal data to that of the European Union. A special action on this purpose was inserted in the National Action Plan for the implementation of the Association Agreement Republic of Moldova - European Union for 2017 -2019, approved by the Government Decision no. 1472 of 30.12.2016, and namely action no. 17 of Article 13 "Preparing for the submission of the application by the Republic of Moldova as a third State ensuring an adequate level of protection of personal data".

Thus, the modification of the legislation of the Republic of Moldova in the field of personal data protection is a major step in order to recognize the Republic of Moldova as a state that ensures an equivalent level of personal data protection with that of the European Union.

The establishment of an equivalent level of data protection is achieved by a European Commission decision, after a thorough analysis of the national legal framework and expertise of the sector in terms of policy of personal data protection: the police sector, education sector, health sector, social welfare, etc., followed by an opinion from the European Data Protection Board.

In this sense, it is important to note that the effects of a European Commission decision on the recognition of the Republic of Moldova as a state that ensures an adequate level of protection of personal data equal to that provided by the EU member countries will generate a wide range of benefits for the Republic of Moldova, including: increasing the credibility of the Republic of Moldova, strengthening the economic strategy, developing the business environment, attracting investments, etc.

During 2017, the NCPDP attended the meetings of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (T-PD and T-PDBUR). In this context, the main subject of interest was the development of a Practical Guide on the Use of Personal Data in the Police Sector, the final version of which was approved on 19 January 2018, of course without decreasing the importance of other acts that are under development (draft Recommendation on the protection of health-related data, Big Data and modernization of Convention 108). The NCPDP was strongly involved in its promotion, the guide being discussed and sent to Moldovan police authorities (Prosecutor's Office, National Anti-Corruption Center, Police, etc.) to disseminate good European practices at national level. In the next period, the NCPDP will request information from the mentioned authorities, the degree of implementation of the Police Guidelines and will provide the necessary support.

MONACO

Développements majeurs intervenus sur les 12 derniers mois en matière de protection des données personnelles à MONACO :

1) textes

PÉRIODE ALLANT DE JUIN 2017 A JUIN 2018

lois votés

n° 1458 - Loi sur l'aviation civile
n° 1457 - Loi relative au harcèlement et à la violence au travail
n° 1454 - Loi relative au consentement et à l'information en matière médicale

Projets de lois déposés

n° 973 - Projet de loi relative au renforcement de la protection des personnes contre la diffamation et l'injure
n° 972 - Projet de loi renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption

Ordonnances Souveraines

Ordonnance Souveraine n O 6.527 du 16 août 2017 modifiant l'Ordonnance Souveraine du 23 décembre 201 5 ayant institué l'Agence Monégasque de Sécurité Numérique ;

Arrêtés Ministériels

. Arrêté Ministériel nO 2018-67 et Arrêté Ministériel nO 2018-68 du 30 janvier 2018 portant application de l'article 54 de la loi nO 1.430 relative à certaines mesures de préservation de la sécurité publique, portant, respectivement, critères de validation de la conformité au Référentiel Général de Sécurité des services d'horodatage électronique et des services de validation qualifiés de signature électronique et cachets électroniques qualifiés ;

- Arrêté ministériel n. 2017-583 du 19/07/2017 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale fixant les conditions de déclassification des informations;

. l'Arrêté Ministériel n° 2017-392 du 26 juin 2017 portant application de l'article 3 de ladite loi 1.430, précitée, relativement à l'énonciation des domaines et activités susceptibles de donner lieu à une enquête administrative ;

. les Arrêtés Ministériels numérotés 2017-576 à 2017-583 qui portent sur les questions afférentes à l'application de la loi 1.430 et notamment, dans ordre de numérotation desdits arrêtés :

- les systèmes de vidéoprotection ;
- les règles d'accès et d'habilitation aux locaux, serveurs et postes de travail utilisant des infomations nominatives
- le contrôle automatique des véhicules automobiles ;
- les opérateurs et prestataires de services chargés de l'exploitation de réseaux et le traitement des demandes transmises à ceux-ci ;
- la mise en service des techniques spéciales d'investigations ;

- les interceptions de correspondances ;
- les techniques d'écoute et de traçabilité dans l'exécution de ces techniques ;
- l'organisation de la commission instituée en article l6 de ladite loi.

3) CCIN - autorité de contrôle - 2017 / 2018 : faits marquants

LES DELIBERATIONS PORTANT RECOMMANDATION

En application de l'article 2 de la Loi n°1.165 du 23 décembre 1993, la Commission a adopté en 2017 quatre délibérations portant recommandation, dont une se substitue à une recommandation formulée précédemment.

Une délibération portant recommandation sur les échanges automatiques d'informations à des fins fiscales

L'échange automatique d'informations a été reconnu au niveau international comme un moyen de lutte contre la fraude et l'évasion fiscales transfrontières. Il consiste à communiquer de manière systématique, entre les Etats liés par des Accords et des Conventions, « *sans demande préalable, à intervalles réguliers préalablement fixés, [des] informations prédéfinies concernant des personnes résidant dans d'autres États membres, à l'État membre de résidence concerné* ».

A cet effet, chaque Institution financière déclarante à Monaco doit transmettre à la Direction des Services Fiscaux des informations concernant chaque « *compte déclarable* » de ladite Institution.

En conséquence, les entités concernées doivent collecter auprès de leurs clients non-résidents des informations relatives à leur identification, à leurs actifs et à leurs revenus financiers qu'elles communiquent ensuite dans un format normalisé à la Direction des Services Fiscaux qui transmet ensuite ces informations aux Autorités de l'État dont le client est résident fiscal, et aux seules fins prévues par les Accords et Conventions précités.

Consultée à ce sujet par différents acteurs publics et privés de la Principauté de Monaco, la Commission a émis une délibération n° 2017-001 du 4 janvier 2017 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *La gestion des obligations légales relatives aux échanges automatiques d'informations à des fins fiscales »* mis en œuvre par les Institutions financières déclarantes.

En effet, elle a estimé nécessaire de guider les responsables de traitement dans l'accomplissement de leurs obligations dans la mesure où ils sont tenus de délivrer aux personnes concernées non seulement l'information figurant à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, mais également, une information complémentaire s'inférant de l'article 1er de la 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.

La nouvelle recommandation relative aux dispositifs d'enregistrement des conversations téléphoniques mis en œuvre sur le lieu de travail par les établissements bancaires et assimilés

En 2017, la CCIN a remplacé sa recommandation n° 2012-118 relative aux dispositifs d'enregistrement des conversations téléphoniques mis en œuvre sur le lieu de travail par les établissements bancaires et assimilés, afin de prendre notamment en compte les évolutions législatives intervenues en matière de prescription à Monaco par le biais de la Loi n° 1.401 relative à la prescription civile.

En effet, aux termes de cette recommandation, les délais de conservation des enregistrements téléphoniques étaient de 10 ans en distinguant deux hypothèses :

« *1. si l'enregistrement des conversations téléphoniques entre dans le cadre de la relation d'affaires entre un établissement bancaire et ses clients, une durée de conservation maximale de 10 ans est suffisante. Cela correspond aux délais de prescription attachés aux actions en justice en matière commerciale (art. 152 bis du Code de commerce) ;*

2. si l'enregistrement des conversations téléphoniques a pour but la détection de crimes ou délits visés aux articles 218-1 et 218-2 du Code pénal, la durée de conservation pourra être au maximum de 10 ans, conformément au délai de prescription prévu à l'article 12 du Code de procédure pénale. »

Or, la Loi n° 1.401 a abrogé l'article 152 bis du Code de Commerce en matière commerciale.

La Commission, constatant que les enregistrements téléphoniques sont uniquement justifiés par l'application de la Loi n° 1.338 relative aux activités financières et son Ordonnance d'application aux fins de traçabilité des ordres, a supprimé les références à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et a ainsi ramené à 5 ans la durée de conservation des enregistrements téléphoniques mis en œuvre par les établissements bancaires.

Adoption d'une recommandation relative à la gestion des contentieux des responsables de traitement

La Commission a constaté que les traitements de gestion des contentieux, légitimes et usuels, ne faisaient l'objet d'aucun encadrement alors même qu'ils peuvent porter sur des soupçons d'activités illicites, des infractions, des mesures de sûreté, devant dès lors être soumis à autorisation préalable de la Commission.

Aussi, cette dernière s'est attachée à définir un cadre clair pour les responsables de traitement qui vont collecter des informations relatives à toutes les personnes intéressées à la procédure.

Ces traitements ont pour fonctionnalités de préparer et suivre une action disciplinaire, une action en justice, et d'effectuer un suivi des décisions rendues pour les faire exécuter.

La Commission a tenu à rappeler que le droit d'accès ne saurait conduire les parties adverses à accéder directement aux documents contenus dans les traitements dont s'agit, notamment ceux couverts par le secret professionnel des avocats.

Enfin, la Commission a fixé les délais de conservation suivants :

- en cas de précontentieux les informations nominatives doivent être supprimées dès le règlement amiable du litige ou à la date de prescription de l''action en justice correspondante ;

- en cas de contentieux, lesdites informations doivent être supprimées dès l'extinction des procédures et de leurs exécutions.

Une nouvelle recommandation pour les systèmes d'habilitation mis en œuvre à des fins de contrôle ou de surveillance

Afin d'aider les responsables de traitement dans leurs démarches auprès d'elle, la Commission a adopté fin 2017, une recommandation précisant les grands principes de protection des informations nominatives applicables lorsqu' un système de gestion des habilitations et des accès informatiques est mis en œuvre au sein d'une entité à des fins de surveillance ou de contrôle.

La Commission a en effet toujours souligné l'importance de sécuriser les systèmes d'information (SI) et de garantir la confidentialité des données que celui-ci contient. Elle recommande donc aux entités de mettre en place un véritable système d'habilitation afin que chaque utilisateur du SI ne puisse accéder qu'aux données dont il a besoin pour l'exercice de sa mission, ce qui se traduit au niveau interne par la

mise en place d'un mécanisme de définition des niveaux d'habilitation d'un utilisateur dans le système, et d'un moyen de contrôle des permissions d'accès aux données.

Cette habilitation doit être fonction d'un profil préalablement défini, généralement lié à une position hiérarchique ou à une fonction au sein de la structure, et non à une personne déterminée. Cela permet de faciliter la gestion des accès en cas de mouvement de personnel. *A contrario*, lorsque les accès sont attribués par personne, il convient d'être extrêmement réactif et de supprimer sans délai tout accès en cas de départ d'un membre du personnel du service ou de la structure.

L'habilitation doit ainsi conférer à chaque utilisateur les droits qui sont strictement nécessaires à l'accomplissement de ses missions. A ce titre, elle doit déterminer, notamment :

- les données et applications auxquelles l'utilisateur peut avoir accès, de manière dédiée ou partagée (réseau local ou partagé, dossiers de travail, imprimantes, téléphones, etc.) ;
- l'étendue des droits ainsi conférés : accès en simple consultation, en inscription, en suppression.

La Commission appelle par ailleurs l'attention des responsables de traitement sur la nécessité de responsabiliser les utilisateurs du SI à la protection de leurs informations nominatives.

D'autre part, dans un souci de transparence envers les employés, ainsi que de loyauté dans la relation de travail, elle demande à ce que le responsable de traitement ou son représentant mette en place une charte informatique, venant préciser, notamment :

- les procédures de contrôle et de surveillance mises en œuvre ;
- la ou les finalités de ces procédures ;
- les personnes habilitées à avoir accès au traitement ;
- la durée de conservation des données collectées ;
- les modalités d'exercice par les personnes de leurs droits d'accès à leurs données.

La Commission insiste également sur la nécessité de mettre en œuvre une sensibilisation de l'ensemble des utilisateurs du SI non seulement sur les habilitations qui leurs sont accordées et des responsabilités qui en découlent, mais également sur le fait que toutes leurs actions sont tracées.

Enfin, en ce qui concerne la sécurité, elle préconise entre autres que l'authentification soit effectuée par un identifiant et un mot de passe individuel réputé fort régulièrement changé, que les accès des personnes habilitées fassent l'objet d'une journalisation et que ces personnes habilitées soient astreintes à une obligation de confidentialité particulièrement stricte, précisée par écrit (par exemple dans une charte informatique, une charte administrateur ou le contrat de travail).

La mise en place d'un tel système impliquant la collecte d'informations nominatives, la recommandation de la Commission s'adresse en conséquence aux personnes morales de droit public ou Autorités publiques qui sont soumises au régime de demande d'avis

Elle s'applique également aux personnes physiques ou morales de droit privé et organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public, visées respectivement aux articles 6 et 7 de la Loi n° 1.165 du 23 décembre 1993, qui sont soumis au régime de demande d'autorisation des lors que ledit système est mis en place soit à des fins de contrôle ou de surveillance, soit dans le cadre de « *soupçons d'activités illicites* ».

A cet égard, la Commission indique que cette notion de contrôle ou de surveillance du système de gestion des habilitations se conçoit comme « *toute activité qui consiste en la collecte, la détection et/ou l'enregistrement, dans le cadre de rapports établis à intervalles réguliers, des données à caractère personnel d'une ou de plusieurs personnes, relatives à l'utilisation des habilitations informatiques* ».

A titre d'exemple, elle considère ainsi que cette définition peut inclure la supervision par le biais d'un système de remontée d'alerte et/ou d'alarme.

En revanche, lorsque le système n'est pas mis en œuvre à des fins de surveillance ou de contrôle, la gestion des habilitations est alors régie par l'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.

12ème JOURNEE DE LA PROTECTION DES DONNEES

Réalisation d'une affiche de sensibilisation aux enjeux de la protection des données personnelles.

Cette affiche au format de 4 mètres sur 3 mètres a été diffusée du 24 au 31 janvier 2018 sur les panneaux d'affichage municipal de Monaco.

4) autre information :

- Sur le portail officiel du Gouvernement, création d'une rubrique dédiée à la protection des données personnelles sur la page "Action Gouvernementale" - "Un État Moderne".-

MONTENEGRO

In relation to the request for information about the undertaken activities of Montenegro in the area of personal data protection between the two conferences, we would like to inform you about the following:

- in April 2017, amendments were made to the Law on Personal Data Protection, which regulate video surveillance of public areas, which were published in the "Official Gazette of Montenegro" number 022/17 of 03/04/2018;

- in January 2018 through a decision of the Minister of the Interior a Working Group was established for the development of the Law on Personal Data Protection, which needs to implement the DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA and the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Through a TAIEX project we asked for the assistance from colleagues from Italy and Slovenia in the development of the new Law. The Draft Law will be subject to a public debate;

- In the Training Centre for Judges, a training of judges was carried out regarding personal data protection within the Project;

- the Agency for the Protection of Personal Data and Free Access to Information in 2017:

➢ performed a total of **117 supervisions** out of which 30 regular supervisions covering the following subjects: private pre-school institutions, public institutions, state bodies, NGOs for helping children and adults with special needs, private medical offices and companies; 65 extraordinary supervisions, as follows: according to the requests for the protection of rights 16 and on the basis of the initiative to perform supervision 49 (forty-nine); one additional supervision was performed at the MoI Police Directorate Podgorica, Sector for Criminal Intelligence Affairs and 21 repeated supervisions - (verification of procedure).

➢ the Agency adopted **18 decisions**, out of which 13 based on the Complaint to the minutes on the performed supervision, where 2 complaints were accepted, 10 complaints were rejected as unfounded and one complaint was partially adopted.

One decision was adopted upon the request for granting approval for video surveillance, rejecting the request as well as one decision rejecting the request for temporary prohibition of personal data processing.

In accordance with its legal authorizations, the Agency adopted two decisions ordering the elimination of irregularities in the processing of personal data.

In the reporting period, one decision was adopted annulling the decision of the Council of the Agency, which ordered the Supervision Department to carry out a repeated supervision.

➢ In the reporting period, **143 records** on personal data filing systems were sent to the Agency's address. Records were provided by **42 controllers**.

The number of controllers and filing systems classified by sector is as follows:

- state body, state administration body and local self-government body 8 controllers (24 filing systems),
- business entities 6 controllers (27 filing systems),
- public institutions and companies 7 controllers (23 filing systems),
- NGO Sector 3 controllers (8 filing systems)

- private medical institutions and laboratory 9 (31 filing systems),
- banks and insurance companies 5 controllers (17 filing systems),
- hotel and hospitality industry companies 4 controllers (13 filing systems).

- Based on the submitted documentation envisaged by the law, the Agency issued **28 approvals** for the establishment of the video surveillance system.

- **49 requests for opinion** were sent to the Agency. Acting upon the requests the Agency adopted 16 opinions regarding the application of the Law on Personal Data Protection. In 7 cases, the Agency gave a positive opinion regarding the implementation of the Law on Personal Data Protection; in 3 cases it gave an opinion that the processing of personal data is not carried out in accordance with the provisions of this Law; in 5 cases an opinion regarding the transfer of personal data from Montenegro and 1 opinion on the Law on Voter Register.
  6 requests for providing opinion were rejected because they related to the protection of personal data in the application of the Law on Free Access to Information. In this regard, the requesters were sent letters indicating that the Council of the Agency, pursuant to Article 38 of the Law on Free Access to Information, is a second instance body dealing with an appeal filed against an act of the first instance body, and hence it can not give opinions on such because there would be a possibility to decide twice about the same matter.

- The Agency prepared and delivered **63 letters** on the inquiries of natural and legal persons regarding the processing of personal data.

- During 2017, the Agency continued to carry out numerous activities on promotion and underlining of the right to protection of personal data. The Agency did this by organizing educational seminars and trainings, participating in trainings or seminars, as well as at round tables, conferences, etc., as well as through the media and other means of communication.

Celebration of the International Data Protection Day

- Secondary Mixed School „Mladost“ Tivat 31/01/2017, educational lecture on personal data protection for pupils
- Secondary Medical School in Berane, 31/01/2017

TAIEX Workshop on "Protection of Personal Data and Free Access to Information", April 3 and 4, 2017 in Podgorica
Panel discussion of the EU Info Center (EUIC) in cooperation with the Agency for the Protection of Personal Data and Free Access to Information "**Data Protection**", Podgorica, July 18, 2017

EU IPA 2014 “International Cooperation in Criminal Justice: Prosecutors’ Network in the Western Balkans” implemented by GIZ and CILC

Within the EU IPA 2014 "International Cooperation in Criminal Justice: Prosecutorial Network of the Western Balkans" implemented by GIZ and CILC, training was organized for state prosecutors and administrative staff on the rules for protecting personal data in the work of the state prosecutor's organization.

Lectures on protection of personal data in Secondary Vocational School - Pljevlja and Secondary School "T. Pejatović "- Pljevlja on September 26, 2017
Lecture to journalists on the topic "Reporting on special categories of personal data and minors in the media", December 1, 2017.

Zora Čizmović, HEAD

MOROCCO / MAROC

Lancement de la bibliothèque virtuelle de la CNDP

En commémoration de la journée mondiale du livre et des droits d'auteur, la Commission Nationale de Contrôle de la Protection des Données à caractère Personnel (CNDP) a mis en ligne sur son site web, une bibliothèque virtuelle dédiée à la Protection de la vie privée et des données personnelles.
La bibliothèque, comprend une centaine de titres sous format PDF, sera enrichie régulièrement dans l'objectif de constituer à terme une référence nationale en matière de documentation spécialisée dans la protection de la vie privée et des données personnelles.
A travers cette initiative, la CNDP vise à :
Contribuer au développement de la recherche en matière de Protection des données personnelles ;Promouvoir la culture de la protection de la vie privée auprès du public ;
Sensibiliser les internautes aux thématiques inhérentes aux activités de la CNDP.

La CNDP approchée par l'autorité judiciaire
La CNDP a été approché pour la première fois par l'autorité judiciaire pour délivrer son expertise. Cette affaire était liée à la fuite de la photo d'une personne depuis le système de vidéosurveillance d'une épicerie. Ladite photo s'est devenue virale sur les réseaux sociaux. La CNDP a mené à cet effet un contrôle sur place pour enquêter sur l'affaire.
Projet d'amendement de la loi 09-08

La CNDP travaille sur le projet d'amendement de la loi 09-08 sur la protection des données ; ce projet permettra de mesurer les écarts par rapport au nouveau règlement européen RGPD ainsi que la convention 108 actualisée et de les intégrer dans la nouvelle loi.

Le Maroc assure le secrétariat permanent du Réseau africain des autorités de protection des données
Lors d'une assemblée générale extraordinaire tenue février dernier en marge de la conférence internationale de la vie privée et de la protection des données personnelles en Afrique, les autorités africaines ont proposé le Maroc pour assurer le secrétariat permanent et pour abriter le siège du Réseau africain de la protection des données personnelles (RAPDP).
Cette décision est venue suite à la modification du statut du réseau afin de lui permettre une gouvernance meilleure. Ces amendements prévoient la création d'un bureau composé du président, de deux vice-présidents et d'un secrétariat permanent.

La CNDP accompagne les entreprises pour la conformité avec le RGPD.
La CNDP a tenu un certain nombre de réunions avec des fédérations professionnelles sur le GDPR.
Au cours de ces réunions, la CNDP a présenté a les principes directeurs du GDPR, son impact potentiel sur la compétitivité de certains secteurs et les actions à entreprendre par les entreprises marocaines pour assurer la conformité.
Il convient de noter qu'une section consacrée au GDPR a été créée sur le site Web du CNDP, résumant les changements majeurs apportés par le règlement et suggérant des ressources utiles à des fins de conformité.
Dans un contexte connexe, le CNDP a publié un communiqué de presse exhortant toutes les parties prenantes à déclencher le processus de conformité du GDPR ; plus de détails peuvent être trouvés sur le lien suivant :
http://www.cndp.ma/images/commpresse/Commpresse-07-09-2017-fr.pdf
loi 31.13 équilibre entre accès à l'information et protection de la vie privée

Le 12 mars dernier la loi 31.13 relative à l'accès à l'information a été publiée dans le bulletin officiel. L'adoption du texte permettra de fixer les domaines d'application du droit d'accès à l'information détenue par l'administration publique, les institutions élues et les organismes investis d'une mission de service public. La loi permettra aussi de définir la nature de ces informations et la procédure de leur obtention, les cas d'exception notamment les données personnelles ce qui va permettre d'assurer un équilibre accès à l'information et protection de la vie privée.

NETHERLANDS / PAYS-BAS

As goes for all EU-member states, the biggest recent development in the field of data protection in the Netherlands has been the introduction of the GDPR. With that, our main concern last year was to get the GDPR implemented in time. Not only with regard to the necessary legislation, but also to make all controllers aware of the new rules and to help them to implement those rules in their day tot day business.

The bill revoking the Data Protection Bill and implementing the GDPR ("Uitvoeringswet Algemene verordening gegevensbescherming" or UAVG) has been adopted by the House of Representatives on March 13th. The bill was adopted by the Senate on May 15th and entered into force on May 25th.

A separate bill that technically adapts our sector-specific legislation to the GDPR has been sent to the House of Representatives April 23rd and is expected to enter into force in the near future. The same goes for the delegated legislation in which technical adjustments are made to existing delegated legislation.

Meanwhile, the Ministry of Justice and Security has started several initiatives to enhance the public awareness about the GDPR especially for (small) businesses. In doing so we have cooperated not only with the supervisory authority in the Netherlands, but also with employers' organizations. They have jointly developed information material aimed at different target groups.

Other major developments are still ongoing and have not yet been completed. This is the case, for example, with regard to the implementation of de PNR Directive and the implementation of the Law Enforcement Directive.

NORWAY / NORVEGE

“The single most important event concerning personal data protection in Norway since the 34th meeting of the T-PD is that in May 2018, the Norwegian Parliament passed legislation implementing Regulation (EU) 2016/679 (General Data Protection Regulation). The legislation, which includes a completely new act for the processing of personal data, is expected to come into effect in summer 2018. “

Øyvind Molven
Acting legal adviser

POLAND / POLOGNE

Country report on major developments in the data protection field

I. Legislation

1. Recent National Developments – legal framework

The new Personal Data Protection Act of 10 May 2018 entered into force as of 25 May 2018. The Ministry of Digital Affairs was the public office responsible for preparing the draft of the Polish Personal Data Protection Act and after several months of consultations the draft was sent on the 5 April 2018 to the Sejm of the Republic of Poland (the lower chamber of the Polish Parliament). There after three readings it was directed to the Senate (the upper chamber of the Polish Parliament) and later to the President of the Republic of Poland. On May 22nd the draft was officially signed by the President and as of May 25th it has become the official Polish Personal Data Protection Act.

The first significant change that this Act introduced was that the Inspector General for Personal Data Protection (GIODO) was replaced by the President of the Personal Data Protection Office as of 25 May 2018. For the purpose of optimum execution of its tasks resulting from the General Data Protection Regulation, the Office has undergone significant structural re-organisation.

Furthermore, it is worth noting that the previous Polish Personal Data Protection Act since 2015 offered the possibility to designate an administrator of information security which was the Polish equivalent of the DPO. With over 25 thousand DPOs designated and registered with the Inspector General it is safe to say that there is a big group of people that have been preparing for the GDPR, no longer upcoming but already here. And the Polish Personal Data Protection Act seeing the importance of the already well established group of professionals created transitional provisions that will help current DPOs. Article 158 of the new Act gives special treatment to DPOs that have been designated before May 25th, allowing them to ex lege become new DPOs until September 1st without any necessary action on the controllers part. Furthermore, controllers who did not designate a DPO before May 25th, but are now obliged to do so, have a special leniency period until July 31st to meet the obligation. All this was introduced to give controllers and processors time to assess their needs and existing staff, establish best practices and allow for a safe period of time within which certain decision can be taken.

As regards derogations from the general GDPR applicability, it is worth noting that the Polish Act does not differ when it comes to conditions applicable to child's consent in relation to information society services, leaving the GDPR suggested age of 16.

However, one example of a significant change is the lowering of potential administrative fines to PLN 100 000 – around EUR 24 000, for public finance sector entities and an even lower amount of PLN 10 000 which is little over EUR 2 000 for state and local government cultural institutions.

And last but not least, it is worth noting that sectoral provisions which are intended to adapt all legal acts to the provisions of the GDPR have been undergoing ministerial and public consultations and have now been directed to the Permanent Committee of the Council of Ministers, after which they will be discussed by the Council of Ministers and then, in turn, the Parliament.

II. Events

On 17 October 2017 the International Conference on the occasion of the 20th anniversary of the personal data protection law in Poland „Unchanging Values and their Effective Protection in the Era of Changes" was organised by GIODO in Warsaw in the Sejm of the Republic of Poland under the honorary patronage of the Speaker of the Sejm of the Republic of Poland. The Conference was attended by over 250 persons – representatives of public administration, including institutions cooperating with GIODO, representatives

of the Hungarian, Bulgarian and Georgian data protection authorities, as well as representatives of the academia, including professors – members of the GIODO Experts Commission.

In 2018, just like in previous years, GIODO celebrated, already for the 12th time, the European Data Protection Day. As each year, conferences devoted to most recent issues related to the right to privacy and data protection were organised by GIODO as well as by universities with which it concluded cooperation agreements in cooperation with GIODO and with active participation of GIODO and/or GIODO's representatives, including inter alia:

22 January 2018, Cracow – the Conference entitled "The GDPR, new provisions, new obligations, a new profession" organised by the Ignatianum Academy in Cracow.

29 January 2018, Warsaw – the main Data Protection Day event organised by GIODO in Warsaw, including the Conference entitled "Invest in privacy! We are getting ready for the #GDPR" devoted to practical aspects of the implementation of the GDPR and the preparation for the beginning of its application, as well as the possibility to obtain educational materials and legal advice on personal data protection provided by GIODO's experts.The Conference also gave an opportunity to award for the first time the 'Michał Serzycki Data Protection Award' established by GIODO to commemorate Michał Serzycki, GIODO of the 3rd term of office, who passed away in 2016. Among the Award winners was Sophie Kwasny, Head of the Data Protection Unit of the Council of Europe. The prize is awarded for promoting data protection values and the right to privacy.

30 January 2018, Lodz – the Poland-wide scientific Conference "The data protection controller from the perspective of the GDRP" organised by the Centre for Personal Data Protection and Information Management at the Faculty of Law and Administration of the University of Lodz.

30 January 2018, Warsaw – the Poland-wide Conference entitled "The Administrator of Information Security in the new role – Data Protection Officer" organised by the Association of Information Security Administrators (SABI) and the Faculty of Management of the Warsaw University of Technology.

1 February 2018, Dąbrowa Górnicza – the Open Day of the Inspector General for Personal Data Protection organised by the University of Dąbrowa Górnicza, including the thematic Conference concerning the new role and practical aspects of the work of Data Protection Officers in the light of the GDPR and the alignment of personal data protection in educational institutions to the requirement of the GDPR. The possibility to obtain educational materials as well as legal advice on personal data protection provided by experts (inter alia from the GIODO Bureau).

2 February 2018, Cracow – the Conference for school principals and teachers entitled "Personal data protection in educational institutions in the light of the GDPR" organised by the Pedagogical University of Cracow.

15 February 2018, Warsaw – the Conference „From the Data Protection Act to the GDPR" organised by the Centre for Research on Social and Economic Risks of Collegium Civitas.

21 February 2018, Wroclaw – the Open Day organised by the Faculty of Law, Administration and Economics of the University of Wroclaw, including the Conference on personal data protection and a possibility to obtain legal advice.

28 February 2018, Gdynia – the Scientific Symposium entitled "Security of personal data in cyberspace – opportunities, challenges and risks" organised by the Polish Naval Academy in Gdynia.

26 February 2018, Warsaw – the meeting of the Senate of the Medical University of Warsaw in connection with the celebration of the Data Protection Day.

27-28 February 2018 – the scientific Conference “Participation of the Police and other services and institutions in the protection of the State critical infrastructure in the era of asymmetric risks. Diagnosis and perspectives” organised by the Police Academy in Szczytno.

Furthermore, in **January/February 2018** 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.

III. Educational activities

Educational activities

The Polish DPA continued its diversified educational activities, in particular aimed at preparation for the implementation of the EU General Data Protection Regulation, for the purpose of increasing awareness of both data subjects and Data Protection Officers, including for example conferences, trainings, workshops etc. (see point II Events above).

In the reporting period, the Polish DPA has conducted training courses for administrators of information security (current Data Protection Officers – DPOs) from the following sectors: medical sector, courts, banking sector, foundations and associations, social services sector, schools and pre-schools.

At the same time, many materials are being developed to help data controllers implement certain duties. In the recent period, materials regarding risk analysis and impact assessment for data protection have been published, as well as an exemplary register of processing activities and a register of processing categories that are to be carried out by data controllers and processors.

The Polish DPA is also responsible for the 8th edition of the essay on data protection competition. The purpose of this competition is to promote data protection among law and administration students, and raise awareness about the upcoming GDPR.

Moreover, in the reporting period the Polish DPA concluded agreements on cooperation on the protection of privacy and personal data with several universities and educational institutions.

Projects and programmes

Within its educational activity, the Polish DPA is inter alia involved in realising EU co-funded projects.

The Polish DPA is one of the partners of the 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.

Moreover, the Polish DPA is a partner of the project financed by the European Commission Erasmus + "e-OpenSpace: European Innovative Open Platform for Electronic Networking and Sustainable Provisions of Adult Centred Education in Privacy and Personal Data Protection". The coordinator of the project is the Bulgarian Commission for Personal Data Protection, and its partners next to the Polish DPA are the Croatian Agency for Protection of Personal Data, the Sofia University St. Kliment Ohridski, the

Jagiellonian University and the Italian Group of Volunteers for Minors and Adults (GVMAS) focused on the future tasks designated to them.

The aim of the project is to create an electronic space - a platform for the exchange of information by data protection authorities as well as the electronic space accessible to all interested parties. This action should provide adults with non-formal education in the area of personal data and privacy protection. The platform will be available through the official website of the data protection authorities, which participate in the project. The project will last 2 years and will end in August 2019.

The Poland-wide Educational Programme „Your Data – Your Concern. Effective protection of personal data. Educational activity addressed to students and teachers" is an undertaking realised by the Polish DPA and the Gliwice Education Centre since 2009. The main objective of the programme is to include the issues related to personal data protection and the right to privacy in the curricula of teachers vocational training centres, primary and middle schools in Poland. From 2010 the programme has its continuation at schools and is realised repeatedly till now; this school year already the 8th edition of the programme is conducted.

PORTUGAL

Relevant Portuguese legislation on personal data protection enacted between November the 24th 2017 and 19th June 2018

- Law 58/2017 of 25th of July
Fourth Amendment to Law 32/2006, of 26 July about medically assisted procreation

This law has specific provisions regarding *consent* (art. 14), *confidentiality* (art. 15), and *register and conservation of data* (art. 16), among many other aspects.

- Law 67/2017 of 9 August
This law regulates the judicial lophoscopic and photographic identifications transposing Council Decisions 2008/615/JHA and 2008/616/JHA of 23rd of June 2008

The provisions of this Law regulate personal data processing lophoscopic and photographic identification. There is a detailed set of definitions and of data processing rules.

- Law 90/2017 of 22nd of August
Second amendment to Law 5/2008 of 12th of February determining the creation of a DNA profile database for civil and criminal identification purposes. First amendment to Law 40/2013 of 25th of June, approving the organisation and functioning of the DNA profiles database Supervision Council.

This law establishes the principles for the creation and keeping of DNA profile databases for civil identification and criminal investigation purposes. There is a detailed set of definitions and of data processing rules.

According to this law, the DNA profile database will contain the profile of nationals, as well as of foreign citizens or stateless persons found or lawfully residing in Portugal.

The processing of DNA profiles, as well as of any personal data, must be carried out in a transparent manner and in strict respect for the private life and informative self-determination, as well as all other fundamental rights, freedoms and guarantees including the principles of authenticity, truthfulness, unambiguousness and safeguard of the identifying elements.

The collection of such data is, as a rule, made based on the free explicit consent of the data subject, an exception being made for minors and disabled persons where both their legal representative and the Public Prosecution have to intervene.

For data subjects under criminal investigation and for convicted persons such data are collected by request of the data subject or by a decision from the judicial authorities. The collection in case of decision from the judicial authority may be compulsory in case of refusal of the data subject.

The data subject is entitled to receive, namely:
- The information that his/her data is going to be inserted in a data file;
- The information about the nature of the data extracted from the sample, that is to say his/her DNA profile;
- The information that his/her DNA profile will be, as provided by law, integrated in a DNA profile database;
- The information of the possibility of the connexion of his/her DNA profile information with other DNA profiles existent in the database, with the reference to the possibility of the use of such data for criminal investigation purposes, if applicable;
- The information that the collected sample may be stored in a biobank.

Requisites of security and confidentiality of information must be fully complied.

A biobank is created to keep the samples for the purpose of analysis and counter analysis necessary for civil identification and criminal investigation."

SENEGAL

COMMISSION DE PROTECTION DES DONNÉES PERSONNELLES

DEVELOPPEMENTS MAJEURS DANS LE DOMAINE DE LA PROTECTION DES DONNÉES

I. Projet réforme de la Loi 2008-12 du 25 juin 2018 portant protection des données à caractère personnel

La CDP a organisé un séminaire les 3-4 mai 2018 sur la réforme de la loi 2008-12 du 25 janvier 2018. L'objectif principal du séminaire était d'harmoniser le cadre législatif et réglementaire du Sénégal avec les meilleures pratiques internationales. Les travaux ont porté sur quatre axes :

- L'Autorité de protection ;
- La conformité juridique des traitements de données ;
- Les droits des personnes concernées ;
- La sécurisation des données.
-

A l'issue des débats, il a été retenu de :

- Le renforcement des pouvoirs de l'Autorité de contrôle (missions, personnel, ressources matérielles, prérogatives de contrôle et de sanction) ;
- La promotion d'outils souples de conformité à côté des formalités préalables ;
- La consécration de nouveaux droits (portabilité, oubli, etc.) et le renforcement des droits existants ;
- La spécification des obligations de sécurité.

II. Sensibilisation sur l'entrée en vigueur du RGPD/GDPR

La CDP a organisé ou participé à un ensemble d'activités de sensibilisation/formation sur le nouveau Règlement Général :

- Formation sur le RGPD à l'occasion de la journée internationale de la donnée à l'attention du secteur public, du secteur privé et de la société civile ;
- Participation à une session de formation organisée par le Conseil des Investisseurs Étrangers du Sénégal (CIES) ;
- Formation d'entreprises privées traitant de données personnelles de citoyens européens.

III. Éducation au numérique

La CDP a poursuivi la mise en œuvre de son programme d'éducation au numérique au profit des élèves, particulièrement, sur les dangers inhérents aux réseaux sociaux.

IV. Protection des données et réforme du Code électoral sénégalais

La réforme constitutionnelle de 2018 modifiant le Code électoral a introduit le système de parrainage citoyen au Sénégal. A cet effet, il est prévu la création d'un fichier de parrainage comportant des données à caractère personnel. La CDP a entrepris de sensibiliser les différents acteurs du processus électoral sur les droits et les obligations des uns et des autres.

Par ailleurs, la CDP a édité un mini-guide sur la protection des données personnelles dans la mise en œuvre du système de parrainage.

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 Ministry of Justice proposed a draft Law in December 2017. However, following numerous comments submitted to the Draft Law by various stakeholders the process has been prolonged and the new draft is not made available to the public, while, new time limit for the enactment of the Law has not been defined.

SLOVENIA / SLOVENIE

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD (2017)

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 2017 the Information Commissioner (IC) initiated 655 inspection cases, 226 in the public and 429 in the private sector. The IC also initiated 105 offence procedures. The offences mainly concerned inadequate data security and traceability of data processing, unlawful collecting and further processing of data, inappropriate anonymization, unlawful video surveillance, direct marketing and disclosure of data to unauthorized users. In 2017 the IC increased the number of planned ex officio supervisions in ministries, public administration bodies, health institutions, with major processors of personal data, travel agencies, trade unions and their associations and societies and their associations.

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 2017 the IC issued 1289 written opinions and clarifications and gave more than 1998 clarifications over the phone. In 2017 more than 100 data controllers have requested prior consultation with the IC regarding legislation, solutions or projects in development. Under PDPA the IC is also competent to conduct prior checks regarding biometric measures (4 cases), transfer of data to third countries (29 cases) and connection of filing systems (16 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 (110 cases). Additionally the IC issued more than 100 opinions on legislative proposals.

B. Information on interesting case-law

1. *Unlawful processing of personal data in database of the Police.*

The IC received several proposals from the Police to initiate a minor offence proceeding, as the internal control procedure revealed, that certain employees, who had access to collections of personal data for the purpose of performing their duties, have processed personal data for other purposes than for those, which they were collected for. The offenders committed the offenses using their personal passwords in the main computer of the Police, where they looked into a certain report of a certain police station, which contained data of a concrete event including personal data of certain individuals. They had no legal basis for such insight. Personal data were collected for a legitimate purpose within the duties of the Police, but the offenders did not deal with any official procedure concerning those individuals.

The IC imposed fines for all described minor offences. Offenses, such as those described above, are considered as an abuse of personal data from official records for private purposes (most often curiosity) and misuse of data, which offenders had access to exclusively for performing their duties. Individuals who have access to collections of personal data must be aware that they can use these data exclusively for the performance of their duties (which they must also prove) and that they are obliged to protect the confidentiality of personal data, which they become acquainted with, while preforming their duties and also after the termination of their function or employment relationship.

2. *Collection of data on reasons for sick leave*

The IC initiated an inspection procedure against employer, who adopted the Rules on the Reduction of Sick Leave (Rules) as basis for the collection of personal data on the health status of employees on the forms, which were annexed to the Rules. IC found that the forms also require the collection of sensitive personal data of employees or data on their health status (such as type of illness or injury and diagnosis), information on their private life habits and the causes of a frequent sick leave, which in addition to the unlawful collecting of personal data also constitutes an excessive encroachment on employees' privacy. The employer, although pursuing goals to improve the health and well-being of employees and to reduce the length of sick leaves, had no basis in the law to collect these data. Besides the consent of employee cannot be the legal basis, because in principle it is excluded in employment relations (due to the subordinate position of the employee or the inequality of powers). Consent as a basis for the collection of personal data in employment relationships can only be discussed in rare situations, when it comes to processing personal data for purposes of performing completely optional, additional activities or processes that can be rejected by the employee without fear, that this will affected the employment relationship. The IC found that described collection of data was not one of the completely voluntary processes that can be refused, since each employee was obliged to fill in the forms (the Rules did not explicitly indicate, that filling the disputed categories of personal data in forms was optional). In conclusion the Rules did not provide the employee the freedom of decision, which personal data he will or is obliged to share.

In conclusion the IC decided, that in the relation to sick leave, the employer may collect information on the movement of the worker (instructions from a doctor on rest or admissible movement) and the estimated time of absence, because without them he cannot act, when there is a suspected abuse of a sick leave, or organize the work or provide the replacement for an absent employee. The data can be obtained from the employee or from his personal physician, who is not obliged to provide data. The employer also has the legal basis for obtaining information on the reason (illness, injuries outside work, occupational disease, occupational injuries, care) for temporary restraint from work, because he needs it for a payroll accounting during the temporary stay, but does not have the legal basis for obtaining a diagnosis of illness or injury. Information on the reason for the sick leave (listed above) up to 30 days is evident from the certificate of sick leave brought by the employee, and in absence of more than 30 days from the decision of The Health Insurance Institute of Slovenia.

3. *Uploading a video of a theft and posting it on Facebook*

The IC was informed that a video of a theft of a car, which was parked on a public area, was posted on Facebook. The IC initiated an inspection procedure against the video surveillance provider because of the suspicion of unlawful recording of a public area and illegal processing (transmission and publication) of personal data.

The IC found that the purpose of publishing the video of the theft was to identify the thief as quickly as possible, although the individual, who posted the video, had already informed the Police, which also seized the recording. The individual has illegally obtained a video from a video surveillance provider, who performs the surveillance over the entrance to the plot, and also captures the road, where the vehicle was parked and from which the car was alienated. The IC urged the individual to remove the disputed video from his Facebook profile, which he did.

The IC also found that the controller did not have the legal basis for transmitting the video to the individual, although his vehicle was alienated. Videos such as this are personal data, therefore, the individual could obtain the video on the basis of the right to access as the data subject, but the controller should have masked the images of other faces (including the image of the thief) on the video before submitting it to the individual. The complete video of a theft can be obtained by the Police. The individual could have obtained the video as an injured party from the Police, but he shouldn’t have published it on Facebook. Individuals who have the status of a client in a particular procedure may obtain information from the files (i. e. administrative or judicial) on the basis of procedural laws, but these data may not be disclosed to unauthorized person (it may be used only for legitimate purposes, for example, to protect their rights before the competent authorities).

In addition, the IC's position regarding video surveillance of a public road was, that a video surveillance that records entrances to his business premises or entrances to a protected area, located along a public road, can also capture a part of the road, the supervision of which is necessary in the nature of the matter, in order to ensure the realization of the purposes for which the video surveillance is carried out (i. e. protection of property, control of entry and exit). Since the video also captures passers-by, thereby encroaching on their privacy, the IC added that he can only check the videos in accordance with the purposes set by the law (regulating the video surveillance) in the light of personal data protections. This means that, in the event of an incident (i.e. damage or alienation of property), an insight into the archive of videos must be recorded, but it is inadmissible to continuously monitor the live image.

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), and gave special attention on developing tools for higher awareness of data protection, mainly with wide range of publications and with consistent media relations (press releases, statements, comments, interviews, press conferences). The IC was also present on the Facebook, trying to raise the awareness of the importance of personal data protection through his profile. Together with the Centre for Safer Internet of Slovenia it covered awareness rising activities for children and youngsters. The experts of the IC also (altogether) conducted 100 free lectures. Last but not least it published new guidelines for Social Work Centres and Data protection impact assessment.

In terms of policy issues the IC has dealt extensively with the new General Data protection Regulation and the accompanying Directive concerning law enforcement sector is the first to be mentioned. It 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.

In the context of the European Data Protection Day 2017 the IC hosted a panel discussion "Rights of individuals and obligations of data controllers in General Data Protection Regulation". 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.

The IC also participated in a number of international events and bodies such as: The Article 29 Working Party, Joint Supervisory Body of Europol (from May 2017 "Cooperation Board"), 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 hosted the first meeting of the »Initiative 20i7« at Bled in May of 2017, attended by high representatives of national data protection authorities from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Kosovo and Macedonia. The high representatives of the data protection authorities joined in »Initiative 20i7« signed the "Declaration of co-operation of Data Protection Authorities in Initiative 20i7" agreeing on regular annual informal meetings of the initiative and active exchange of expert opinions, experiences and best practices with the aim of addressing common challenges encountered in protection of personal data.

SWEDEN / SUEDE

- The Swedish parliament has adopted the new data protection act containing provisions that supplements the GDPR. The act was published on 24 April 2018 and entered into force on 25 May 2018. https://www.svenskforfattningssamling.se/doc/2018218.html

- Several laws adapting sector specific data protection rules to the GDPR have been adopted by the Swedish Parliament.

http://www.riksdagen.se/sv/aktuellt/2018/apr/19/sa-paverkar-dataskyddsforordningen-svenska-lagar/

- A Government bill regarding the implementation of the LED was submitted to the Riksdag (Parliament) on 19 April 2018. According to the Government's proposal the new act will enter into force on 1 August 2018.

Développements majeurs survenus dans le domaine de la protection des données

Le 15 septembre 2017, le Conseil fédéral a adopté, à l'attention du Parlement, un projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales. L'objectif de ce projet est en particulier de renforcer la protection des données, notamment par une amélioration de la transparence des traitements et un meilleur contrôle des personnes sur les données qui les concernent. Il doit permettre à notre législation de répondre aux défis de la numérisation de la société et de tenir compte des réformes du cadre juridique européen. A cet égard le projet transpose la directive 2016/680 dans le domaine de la coopération en matière pénale Schengen, permet de se rapprocher des exigences du Règlement 2016/679 et met en place un cadre juridique adéquate pour que la Suisse puisse ratifier le protocole d'amendement à la Convention 108. La révision doit aussi contribuer à maintenir la reconnaissance par l'Union européenne du niveau de protection adéquat de notre pays. La Commission parlementaire du Conseil national (1ère chambre) a décidé, en janvier 2018, de scinder le projet du Conseil fédéral, et a opté pour une approche en deux phases. Dans une première phase la commission a abordé la transposition de la directive 2016/680 et adopté une loi de protection des données Schengen, qui sera traitée au Conseil national le 12 juin prochain. Elle abordera ensuite la révision totale de la loi fédérale sur la protection des données. Parallèlement les cantons ont entamé les travaux de révision de leur législation de protection des données.

Le projet de révision améliore la transparence en matière de traitement des données ; le devoir d'information lors de la collecte est en effet étendu à tous les traitements dans le secteur privé, indépendamment de la nature des données. Le projet introduit un devoir d'information en cas de décision automatisée lorsque celle-ci a des effets juridiques sur la personne concernée ou l'affecte de manière significative. La personne concernée a alors en principe le droit de faire valoir son point de vue et de demander que la décision soit revue par une personne physique, ainsi que de connaître la logique qui sous-tend au traitement. Il permet également l'introduction d'une obligation de procéder à une analyse d'impact relative à la protection des données pour les projets qui présentent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. L'extension de l'obligation d'informer les personnes concernées sur leurs droits d'accès est également ancrée dans le projet. Il en va de même de l'encouragement de l'autoréglementation, par le biais de codes de conduite qui visent à faciliter les activités des responsables du traitement et à contribuer au respect de la législation. Le projet prévoit aussi l'obligation d'annoncer les violations de données, ainsi que l'introduction explicite des principes de la protection des données dès la conception et par défaut. L'indépendance et les pouvoirs du préposé fédéral à la protection des données et à la transparence sont en outre renforcés. Il pourra en effet à l'avenir prendre des décisions contraignantes à l'égard des responsables du traitement et des sous-traitants, au terme d'une enquête ouverte d'office ou sur dénonciation. Le projet ne prévoit pas à ce stade l'introduction d'un droit à la portabilité des données, ni l'introduction expresse d'une obligation de démontrer la mise en conformité. Les sanctions prévues sont des sanctions pénales (amende de 250 000 francs au plus) et non des sanctions administratives.

Le projet de loi et le message du Conseil fédéral peuvent être consultés sur :
/https://www.bj.admin.ch/bj/fr/home/aktuell/news/2017/ref_2017-09-150.html

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

The new General Data Protection Regulation (GDPR) has ushered in a new era of data protection, designed for the digital age. It is an outstanding achievement for the EU, its legislators and stakeholders, but the EU's work to ensure that data protection goes digital is far from finished.

The EDPS Strategy 2015-2019 guides EDPS work and is designed to address the current period of unprecedented change and political importance for data protection and privacy, both in the EU and globally. Our principal aim is to work in close cooperation with our data protection partners to help the EU to lead by example in the global dialogue on data protection and privacy in the digital age.

EDPS Strategy 2015-2019

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

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

1 Data protection goes digital

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

(2) Identifying cross-disciplinary policy solutions;

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

2 Forging global partnerships

(4) Developing an ethical dimension to data protection;

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

(6) Mainstreaming data protection into international policies.

3 Opening a new chapter for EU data protection

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

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

(9) Facilitating responsible and informed policymaking;

(10) Promoting a mature conversation on security and privacy

Overview of Activities

As the supervisory authority for the EU institutions and bodies, we have continued our work carrying out inspections, issuing prior check Opinions and developing our relationships with the DPOs who are responsible for ensuring compliance with data protection law within their respective EU institutions.

However, EDPS cooperation with our data protection partners in the EU institutions has intensified in recent years, as we endeavour to ensure that the EU institutions will be ready for the new data protection rules which will apply to their activities from late 2018 onwards. In particular, we have focused our efforts on introducing them to new and less familiar concepts, such as accountability, Data Protection Impact Assessments (DPIAs), data breach notifications and data protection by design and by default.

However, our work goes further than this. The four areas outlined below provide an insight into the major developments in data protection for the EDPS since June 2017.

Preparing for a new legislative framework

The EU's data protection rules have long been regarded as a gold standard across the world. In the EDPS Strategy, we pledged to support the EU in its effort to develop a new data protection framework designed for the digital era. This has meant offering advice and support to the European Parliament, Council and Commission, to ensure that the EU delivers a practical and coherent data protection reform package, and supporting our data protection partners across the EU, to ensure the correct, consistent and timely implementation of new rules.

- In line with our Strategy commitments, we worked in close cooperation with DPAs across the EU to prepare for the GDPR, in particular by contributing to the Article 29 Working Party's efforts to provide guidance on key provisions of the GDPR.
- The European Data Protection Board (EDPB) succeeded the Article 29 Working Party on 25 May 2018, as foreseen under the GDPR. As the new legal framework specifies that the EDPS should provide the secretariat for the EDPB, we worked hard throughout 2017 and early 2018, and in collaboration with our fellow EU DPAs, to ensure that the EDPB was operational from 25 May 2018. The secretariat will provide the EDPB with administrative and logistical support, as well as perform analytical work contributing to the tasks of the EDPB.
- On 23 May 2018, the European Parliament and the Council reached an agreement on new data protection rules for the EU institutions and bodies. The revised rules on data protection in the EU institutions agreed upon by EU lawmakers bring Regulation 45/2001 in line with the high standards of data protection provided for in the GDPR. As the authority responsible for supervising data protection in the EU institutions, we have been working in close collaboration with DPOs, staff members and top management from the EU institutions and bodies to ensure that they are prepared for the new rules. In particular, our efforts have focused on the principle of accountability.

Supervising Europol

Europol is the EU body responsible for supporting the law enforcement authorities of the EU Member States in the fight against serious international crime and terrorism. Since 1 May 2017, the EDPS has taken over responsibility for supervising the processing of personal data relating to Europol's operational activities. To help us in this role, we work closely with national supervisory authorities through a Cooperation Board, an advisory body for which the EDPS also provides the secretariat.

Some activities of note from our first year as the data protection supervisor for Europol include:

- Establishing a close working relationship with the Europol DPO and Data Protection Function team.
- Providing recommendations in the form of an Opinion on Europol's Integrated Data Management Concept Guidelines (IDMC). These Guidelines set out the procedures according to which Europol must carry out all future processing of personal data under the Europol Regulation.
- Carrying out an inspection at Europol, which took place from 12-15 December 2017 and in collaboration with an expert from the Italian DPA. This inspection focused on the implementation of pending recommendations and an assessment of Europol's overall level of compliance.

Security and EU borders

In the EDPS Strategy, we commit to facilitating responsible and informed policymaking in all cases where EU legislation has a notable impact on privacy and data protection, as well as to promoting a mature conversation on security and privacy.

In recent years, the Commission has proposed several initiatives aimed at ensuring that EU borders, both on land and online remain safe and secure. Though we fully support these efforts, it is vital to ensure that all proposals fully respect the fundamental rights of those concerned. Some areas in which we have provided legal analysis, guidance and recommendations include:

- The EDPS Opinion on the proposal for a Regulation on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA).
- The EDPS Opinion on the proposal for a Regulation on the European Criminal Records Information Service for Third Country Nationals (ECRIS-TCN).
- EDPS Formal Comments on the *Cybersecurity Package* adopted by the European Commission.
- The EDPS Opinion on the proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.

The International Conference and Digital Ethics

On 13 March 2017, it was announced that the 2018 International Conference of Data Protection and Privacy Commissioners (ICDPPC 2018) would be jointly hosted by the EDPS and the Commission for Personal Data Protection of the Republic of Bulgaria.

The EDPS Strategy outlines our commitment to developing an ethical dimension to data protection. We wanted to explore whether regulating the digital world requires an ethical approach and the ways in which such an approach might be developed and implemented. The open session of the 2018 International Conference will therefore focus on Digital Ethics. It will build on the work of the Ethics Advisory Group, set up by the EDPS in 2016, to explore how data and those who control it are influencing our values.

The website of the 2018 International Conference was launched in March 2018. Although digital ethics is not a conventional theme for the ICDPPC, the EDPS believes that, as first-hand witnesses to the digital revolution, data protection regulators and authorities should take the leading role in determining what our common values are and how we can protect them in the digital world. The conference will aim to facilitate dialogue across a wide spectrum of groups and individuals from a range of disciplines.