COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 11 June / juin 2019

T-PD(2019)Mos

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 in the data protection field

/

Information sur les développements recents intervenus dans le domaine de la protection des données

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

TABLE OF CONTENTS / TABLE DES MATIERES

ABU DHABI AND THE U.A.E / ABU DHABI ET LES E.A.U.

Abu Dhabi Global Market

- September 2018: ADGM Registration Authority (containing the Office of Data Protection) became an Observer of the Consultative Committee of Convention 108.
- March 2019: ADGM Office of Data Protection organized and held 'Data Protection in the Middle East' event as part of data protection awareness raising efforts.
- March 2019: ADGM Office of Data Protection issued report on the results of its thematic review of firms in its jurisdiction regarding Privacy Accountability.
- The report is available here: https://www.adgm.com/-/media/project/adgm/operating-in-adgm/office-of-data-protection/documents/dp-thematic-review-report-on-accountability-final-2.pdf

United Arab Emirates

- February 2019: the UAE Federal Government published UAE Federal Law No. 2 of 2019 concerning the use of information and communication technology in the area of health (the "Health Data Law").
- The Health Data Law came into effect in May 2019 and applies across the UAE.
- The Health Data Law regulates how electronic data in the healthcare sector is maintained, secured, accessed and retained reflecting several principles found in data protection laws.
- Penalties for breaches include fines of up to a maximum of AED 1 million.

ALBANIA / ALBANIE

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

REPORTING PERIOD (MAY 2018 - JUNE 2019)

Complaints

Over **210** complaints have been lodged during this period, of which **205** complaints were in compliance with the Law "On the Protection of Personal Data"
For the equitable and full processing of complaints, administrative inspections were carried out with various controllers as well as all procedural steps have been followed, such as continuous communication with the complainants and the data controllers in order to collect relevant information and evidence.

The scope of complaints mainly focused on:

I. Direct marketing with reference to unsolicited communications via telephone or email;
II. Dissemination of personal data in the media and the online portals;
III. Violation of personal data subjects' rights;
IV. Use of cameras in public and private areas;
V. Retention of personal data beyond the specified purpose for their collection.

Notification

131 data subjects have notified in compliance with the legal requirement, totalling **5582** of processing notifications made by controllers in the Republic of Albania**.**

Administrative investigations

The Commissioner's Office has carried out **114** on-site inspections in Tirana, and in other districts; of which **69** with public controllers and **45** with private controllers. Inspections were initiated based on complaints (34), and *ex officio* (80).

Main sectors under scrutiny were:

- Various public bodies;
- Municipalities;
- Private pre-university education;
- Institutions for execution of criminal judgements;
- Ministry of Health;
- Ministry of Education;
- Bailiffs;
- Assets Evaluation Offices;
- Water Supply – Sewage
- Private medical clinics.

The scope of enquiries related to

- *"Adherence to the Law No. 9887, dated 10.03.2008 "On Personal Data Protection", as amended, and its implementing bylaws*".
- *Follow-up audits verifying that the recommendations of the Commissioner were acted upon.*

Upon completion of the administrative enquiries, **30** hearing sessions were held, thereby observing the right of subjects to be heard pursuant to Law No. 44/2015 "Administrative Procedure Code of the Republic of Albania", which resulted in formal decision notices rendered by the Commissioner's Office.

Recommendations

The Commissioner, in accordance with the competences conferred by Law No. 9887/2008 "On the Protection of Personal Data", has rendered **35** recommendations both for public and private controllers.

Administrative Sanctions

Following administrative investigations conducted mainly *ex officio* or on complaint basis with various public and private controllers, the Commissioner's Office has imposed sanctions with punitive fine in cases of serious and recurrent violations, or in case of failure to act upon the Commissioner's recommendations/orders.

The Commissioner's Office has issued **35** decisions with punitive fine, corresponding to **80** administrative sanctions.

International transfer

A total of **11** requests for permission to transfer personal data to a foreign country have been dealt with, and **2** decisions on permitting international transfer have been issued.

Legal Framework

Over the reporting period, the Commissioner has adopted the following instructions:

- Commissioner's Instruction No. 47, dated 14.09.2018 "On determining the rules on safeguarding personal data processed by large processing entities", published in the Official Journal No.137, dated 25.09.2018;
- Commissioner's Instruction No. 48, dated 14.09.2018 "On certifying the information and personal data security management systems and their protection", published in the Official Journal No.137, dated 25.09.2018.

Co-operation/Meetings

Several staff trainings were held in the frame of the activities of the "EU-Albania Anticorruption Twining Project" dealing with the themes of:

"Data protection officers and Codes of Conduct under the General Data Protection Regulation" which gathered, inter alia, representatives of the Bank of Albania, the General Prosecutor's Office and the Power Distributor Network Operator;

"Transparency aspects in the EU General Data Protection Regulation (GDPR)".

Both events featured a speaker from the German Federal Data Protection and Freedom of Information Authority, and were organised in the frame of the "Albania-EU Anti-Corruption Twinning Project

Three national institutions for human rights in Albania, the People's Advocate, the Information and Data Protection Commissioner and the Commissioner for Protection from Discrimination signed a co-operation memorandum, which was drafted under the coordination and with the assistance of the OSCE Presence in Albania. This memorandum aims at strengthening inter-institutional co-operation according to the applicable legislation with relevance to their specific activities in order to boost effectiveness in upholding human rights and fundamental freedoms by public administration bodies and beyond.

Awareness-raising

In the frame of 28 January, the following activities were organized:

"Play and learn – Happy Onlife" is the latest initiative of the Information and Data Protection Commissioner's Office aimed at raising the awareness of children and young people for a safe use of digital environment. In co-operation and co-ordination with the Education Directorate of Tirana, this interactive game intended for the group age 8-14, is being promoted at six 9-year schools of the capital. In 2015, the "Happy Onlife" game was launched by the European Union Joint Research Centre's section in Ispra, Italy. The purpose of this game is the effective protection of privacy and personal data through the exchange and critical thinking of knowledge on digital environment. It points at raising awareness among children and young people, with special focus on the parents and the teachers, in preventing negative phenomena such as bullying, identity theft or unwanted communications.

The Office of Information and Data Protection Commissioner in co-operation with "Epoka" University organized training under the theme "Information and Privacy", gathering students and academics as well as administrative staff of the University. The event provided an insight on the Albanian legislation on personal data protection and the activity and competences of the Office of the Commissioner. The training module introduced the innovations brought about by the EU General Data Protection Regulation (GDPR), and discussed the obligations of data controllers operating in the sector of higher education (both public and private).

Publications

The Office of the IDP Commissioner has issued 3 new editions of its Magazine "Information and Privacy", as well as a flier promoting the awareness on the EU General Data Protection Regulation (GDPR).

International Conference of Data Protection and Privacy Commissioners (ICDPPC)

21-24 October 2019, Albania

The IDP Commissioner's Office will host the 41st International Conference of Data Protection and Privacy Commissioner (ICDPPC) from 21-24 October 2019 in Tirana, Albania. The 41st ICDPPC will hold its Closed Session on 21-22 October, whereas the Open Session will take place from 23-24 October 2019 The dedicated website of the conference was launched earlier in May and is accessible at: https://privacyconference2019.info. A Programme Advisory Committee was established in order to develop the content of the Open Session, and its expert line-up reflects both the balance of interests of the stakeholders attending the Conference and the need to provide substantial input for the conference programme. More information could be sought by emailing privacyconference2019@idp.al.

ANDORRA / ANDORRE

Legal developments

Over the period of time reported here (2018-2019) Andorra has implemented several regulations that have had an impact on the data protection regulation. We can see that there are some mofifications or new regulations that have a direct impact as they develop features that weren't specified in the Data Protection Act. Other regulations instead, introduce new obligations to data controllers in the exchange or communication of data.

From the first category we can find the Qualified Act 14/2019 of Children and Adolescents' Rights that establishes that the legal age in order to consent to data treatments is 16 (prior to this Act, the consent was only valid if the data subject was over 18 years old).

Another example is the Qualified Act 12/2019 of Assisted Reproduction Techniques that in its article 3 gives legal definitions to 'genetic data' and 'informed consent' (where the Data protection Act only defines 'consent' and 'health data').

From the second category, this is new regulations that introduce new obligations to data controllers, we can find several examples.

For instance, the Labour Relations Code that has implemented the obligation of current and past personel to keep confidenciality and secrecy about all information that they may have had acces due to their work.

Also, in July 2018 there was a modification in the Act on the automatic exchange of tax data, introducing the legal consequences of failing to communicate these data to the national supervisor. The modificaction also specified which data should the local public powers communicate to the national supervisor in cases concerning local tax data.

Moreover, the Volunteering Legislative Decree of 2019 introduced the right of all volunteers to have their privacy and personal data protected.

In this category, it should be noted that in different new regulations an explicit submission to the Data Protection Act was added. In October 2018 for example, the Act on Local Administrations' Exchange of Data was modified in order to emphasize the adherence of this act to all the principles and guarantees of the Data Protection Act in the exchange of information between local public powers. Similar is the case of the Act on organs, cells, tissue and blood that submits itself to the Data Protection Act and also creates an independent Authority that will ensure the respect to Data Protection Principles. Furthermore, this Act creates a new procedure of collecting consent, confidenciality and the existence of a National Register of donnors which will also abide to this regulation. Finally, another example of an explicit submission to the Data Protection Act can be found in the Gambling Act.

Consulting Tasks

One of the Data Protection Authority's functions is to participate and give its views on the development of new regulations that may have an impact on Data Protection.

During the period of time analysed in this report, the Andorran Data Protection Authority has participated as an advisory body in the Implementing regulation on the Shared Medical Records System and the modification of the Administrative Code.

Awareness-raising activities

At the occasion of the European Data Protection Day 2018, the Andorran Data Protection Authority published easy and accessible Guidelines about the rights of any data subject paying special attention to those new rights introduced in European Regulations. These guidelines are also available on our website (link below).

In 2019, the Andorran DPA renewed the content of its website paying special attention to a full renovation of the content addressed to youth.

Also, in 2019 the Andorran DPA created a Twitter account in order to give periodical feedback about its activities but also to give short recommendations or guidelines to its followers.

For more information, please consult the Internet site of the Data Protection Authority on www.apda.ad (in Catalan only).

ARGENTINA / ARGENTINE

Introduction

This report summarizes the main advances regarding data protection in Argentina since May 2018. Its aim is to describe, succinctly, the most relevant actions, measures and projects carried out by the Access to Public Information Agency (hereinafter the Agency or the AAPI)[1], which is the federal data protection authority of the country.

Argentina's accession to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Argentina has become the 54th Party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter Convention 108) and the 3rd Latin American country to accede to it. The instruments of accession to the Convention 108 and to its Additional Protocol were submitted to the Secretary General on 25 February 2019. Accordingly, Convention 108 and the Additional Protocol will enter into force on the first of June 2019.

Moreover, and most recently, Argentina has formally initiated the process to sign the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, better known as Convention 108 +. The AAIP in its note to the Ministry of Foreign Affairs and Worship, highlighted the need and importance of becoming a party of the modernized version of Convention 108.[2]

A new data protection law

Technological changes that have taken place during the last eighteen years as from the enactment of the National Data Protection Law[3] (October 2000) together with the new international legal context, principally with the adoption of the EU Data Protection Regulation (hereinafter GDPR), have driven the AAIP to elaborate in 2016 a Draft Bill to reform the current law.[4] The original Draft Bill was partially modified by the Executive before it was to the National Congress in September 2018.[5]

The Draft Bill major goal is to provide a high level of data privacy, adapting to the new international standards on data protection, and, at the same time, enabling further innovation and investment in Argentina.

Interpretation and application of the current law by the AAIP´S resolutions

While the Draft Bill is being analyzed by the National Congress, the Agency has issued a series of resolutions in order to address the challenges presented by the ever-changing technological circumstances and the entry into force of the GDPR. Below is a list of the more relevant resolutions since May 2018.

---

[1] Its name in Spanish is "Agencia de Acceso a la Información Pública".

[2] NO-2019-01978006-APN-AAIP.

[3] See National Law No. 25.326.

[4] See the First Draft, as it was originally written by the AAIP.

[5] See the Second Draft (MEN-2018-147-APN-PTE).

- **Procedure.** As from September 2017, the AAPI has become the Argentine data protection authority as well as the public information agency (Decree No. 746/2017 and No. 899/2017). Resolution No. 5/2018 establishes the internal procedure by which the National Directorate of Access to Public Information and the National Personal Data Protection Directorate must interact when responding to claims or inquiries that involve both Laws No. 25.326 on Personal Data Protection and Law No. 27.275 on the Right to Access Public Information.
- **Privacy policies for the public sector.** Resolution No. 40/2018 sets forth recommendations to enhance protection of personal data in the public sector.
- **Security measures.** Resolution No. 47/2018 sets forth security measures recommended to protect personal information processed digitally and analogically.
- **Binding corporate rules.** Resolution No. 159/2018 sets forth guiding principles and basic content for binding corporate rules.
- **Guiding principles on data protection.** Resolution No. 4/2019 sets forth guiding principles to interpret Law No. 25.326. In brief, the resolution establishes principles to interpret: the right of access to personal data collected by means of video surveillance systems, automated decision-making, dissociated data, biometric data, the general conditions for consent, the conditions applicable to the transfer of data within the public sector and the conditions applicable to child's consent in relation to the processing of their data.
- **Guidelines on data processing for electoral purposes.** An upcoming Resolution by the AAPI sets forth guiding principles for the processing of data with electoral purposes. The document is especially aimed at political parties, candidates, consultants and think-tanks, and includes standards regarding the monitoring of personal data in social networks, the uses of automated mailing and any affiliate registration done by political parties.

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

- the publication and entry into force of our new comprehensive data protection legislation : « loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » published in our Official Journal of September 5th 2018
- the nomination of the new Board of Directors of the principal Data Protection Authority in April of this year.

BULGARIA/ BULGARIE

INFORMATION ABOUT THE DEVELOPMENTS IN THE PERSONAL DATA PROTECTION FIELD- BULGARIAN COMMISSION FOR PERSONAL DATA PROTECTION

From June 2018 till 30 May 2019, the Bulgarian Commission for Personal Data Protection aimed at further developing the personal data protection rules and assisting all the interested parties in the interpretation and application of the GDPR and Directive 2016/680, namely:

1. Amendments and Supplements to the Personal Data Protection Act (PDPA)

The CPDP prepared draft Act on amendament and supplement of the PDPA in order to ensure the implementation of those GDPR provisions left to the MS compence and also to transpose Directive (EU) 2016/680 on the processing of personal data in police and criminal justice activities. Considering the above, in the drafting process participated also the Ministry of Interior, which ultimately was competent for initiating the proposed legislative amendments and leading the approval procedure.

The draft law, introduced measures for the Regulation implementation and laid down both the matters, which the Regulation has left the Member States with the freedom to decide whether and to what extent to regulate them and the issues, which require the explicit introduction of national legislative measures.

In terms of structure, the draft Act:

- repeals a number of texts of the current PPDA, which are now explicitly regulated in the General Data Protection Regulation and the related rules are directly applicable (principles, individuals' rights, data controllers' obligations, transfers of personal data to third countries);
- amends and updates rules in line with the philosophy and spirit of the General Data Protection Regulation (tasks and powers of the CPDP in its capacity as a supervisory authority, exercise of rights of data subjects, remedies);
- formulates new texts the need for which arises out of Regulation (EU) 2016/679 (striking a balance between the protection of personal data and the freedom of expression and information, processing of personal identification numbers, processing of personal data in the context of employment, processing for archiving purposes in the public interest, scientific, historical research or statistical purposes, protection of professional secrecy);
- provides provisions that transpose the provisions of Directive (EU) 2016/680 into national legislation (Chapter 8 of the draft Act).
- The final draft Act, after the conduct of a set of expert and public consultations includes:
- the minimum amounts of administrative fines and penalties were removed;

- the protection of professional secrecy was regulated and situations, in which, the exercise of the investigative powers of the CPDP might lead to the disclosure or breach of such secrecy, as well as of sources of journalistic information, were prohibited;
- the processing of the PIN as the sole identifier for the provision of public services electronically by remote access was prohibited;
- the derogations to the rights of data subjects and the obligations of the data where Regulation (EU) 2016/679 so permits (e.g. for the purposes of national security, defence and public order and security; for the investigation of criminal offences or the execution of criminal penalties; for other important objectives of general public interest, in particular an important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security; for the protection of judicial independence and judicial proceedings; for the protection of the data subject or the rights and freedoms of others; for the enforcement of civil law claims);
- the hypotheses of processing personal data for the purposes of archiving in the public interest, scientific and historical research, statistical purposes, journalistic purposes, humanitarian purposes and disaster situations were legally regulated.

The Amendments and Supplements to the PDPA were adopted by the National Assembly on 20 Feburary 2019 and after promulgation the Act entered into force on 26 February 2019.

2. Publication and Dissemination of CPDP's practical GDPR guidelines

2.1. Information brocures with practical advises

In order to support the GDPR practical implementation, CPDP published on its website a document containing ten practical steps for the Regulation's implementations. The document has purely informational purposes, is not binding and does not pretend to be exhaustive. Its purpose is to synthesise in a comprehensible language the steps that each PDC needs to take in order to bring its data processing activities in line with the new data protection legal framework requirements. In addition to providing website access, the Commission has distributed more than 14 000 paper flyers that contain practical advice and guidance on the General Data Protection Regulation implementation.

On the occasion of the 2019 Data Protection Day, CPDP has issued and disseminated an additional information brochure "New moments in the individuals' personal data proctection rights under the Regulation 2016/679". The main issues, explained in the documents, were the data subjects' rights; the information which the individual should receive from the personal data controller/ processor, when submitting his/her personal data; the request for deletion/ restriction of data from the controller/processor; the new data portability right; the right to object to personal data processing for direct marketing purposes etc.

2.2. Publication on the CPDP's website of useful information concerning the GDPR interpretation and guidance on the new requirements, individuals' rights and data controllers/processors obligations.

- The Data Protection Officer - role, tasks, responsibily, qualifications and cases, as well as the notification form which should be filled and sent. Information is provided, also, on the necessary actions to be taken in case of change in the submitted form or circumstances, following the DPO appointment.
- Cases for which the consent is inapplicable as ground for lawful data processing
- Following the procedure set in Art. 64 of the GDPR CPDP adopted and published an exhaustive list of data processing operations, which require personal data impact assessment.
- In July 2018, CPDP adopted and published criteria and procedures for Codes of Conduct approval in order to facilitate the uniform understanding and application of the new possibility to prepare and use Code of Conduct.
- Jointly with the Central Election Commission, and following the EC guibndance in the topic, CPDP adopted and published "Instructions on the processing and personal data protection during the election process" which were a useful tull for the last EP elections.

3. The 40th International Conference in 2018

Following more than a year of preparatory work, between 22 and 26 October 2018, the CPDP organised the most important international annual personal data protection forum, together with the European Data Protection Supervisor (EDPS) – the International Conference of Data Protection and Privacy Commissioners (ICDPPC). The conference has been held since 1979 and is the largest and most significant annual event for exchange of experience, good practice and analysis of trends in the personal data protection sector, bringing together 121 accredited organisations worldwide. The hosting of the conference is entrusted to countries with proven experience and capacity in the area of personal data protection and respecting human rights and freedoms.

The conference includes a closed session for accredited members and observers and an open session and additional events for all registered participants – a wide audience from the privacy and data protection community, industry, civil society, academia, government bodies and non-governmental organisations.

The jubilee edition of the conference in 2018 was special for a number of reasons. Sofia was the first capital on the Balkan Peninsula, and the Republic of Bulgaria was only the second country after Poland from Central and Eastern Europe to host the forum for almost 40 years. For the first time in the history of the conference, the seminar programme was held simultaneously in two different locations – in Sofia and Brussels, and was organised jointly by a national supervisory authority and a European institution.

The 40th International Conference contributed to the development of the discussion on the ethical dimensions of personal data processing in the digital age and was conducted under the title 'Debating Ethics: Dignity and Respect in Data Driven Life'. The conference outlined how the digital age changes society, how it influences the values and everyday life of people, how dignity and respect can be maintained in a technology-oriented world of digitised societies and economies.

A representative of the CPDP participated actively in the closed session held on 22 and 23 October in Brussels and attended by 350 representatives of accredited members and observers. Issues related to the management of the forum and its future, recommendations and scenarios for its further development and relevance were discussed. The working parties reported on the work done and their plans for the future.

Declarations and resolutions of the 40th conference were presented, discussed and voted. A presentation was made on the next 41st conference to be held in 2019 in Tirana, Albania. The possible hosts the 42nd edition of the conference, which will take place in 2020, were explored. It was officially announced that the 42nd conference will be held in Mexico. The closed session discussed issues relating to the implementation of the General Data Protection Regulation, ethics and data protection in artificial intelligence systems.

The programme in Sofia was targeted at businesses, the non-governmental sector and academic circles. The six plenary debates as well as the accompanying events were intended for over 200 registered participants. Moderators, lecturers and participants in discussions included representatives of Bulgarian, European and international institutions and organisations — the Council of Europe, the European Commission, Europol, the European Data Protection Supervisor, the State e-Government Agency, the Communications Regulation Commission, the Ministry of Interior and others. Representatives of the supervisory authorities of Spain, the Russian Federation and Japan, as well as of the International Association of Privacy Professionals (IAPP) were present. The Bulgarian NGOs were represented by the Access to Information Programme, the Law and Internet Foundation and the LIBRe Foundation. The presence of representatives of the business community was especially pronounced. Attendants included Nymity, OneTrust, Amatas, AT&T, EY, Inveo Srl, Cisco, Sophia Lab, Telelink, Software Group, Sensika Technologies, Euroins Insurance Group, SAS, CENTION profesioal IT security, Vilivosoft and I&S Vassilev, Vivacom, European Investment Bank, Municipal Bank, UnitedLex Corporation/Marshall Dennig and others.

The topics of the plenary discussions that formed part of the conference programme in Sofia were as follows:

- 'Privacy and Human Dignity: Universal Values in a World without Borders', which presented the modernised Convention No 108 as the new global framework for data security and data protection, as well as the European Commission's decision on the adequate level of protection provided by Japan. Participants were particularly interested in the positions expressed by the representatives of Japan, Russia, the European Commission and others.
- 'Balancing Between Public Interest and Data Subjects' Rights' brought together the views of supranational organisations, private businesses, academia and the non-governmental sector.
- 'Smart Solutions for Data Security and Accountability' enabled participants to learn about up-to-date solutions to ensure compliance with the General Data Protection Regulation.
- 'Digital Ethics in the Age of Global Communications and Virtual Reality' – consecutive presentations presented solutions on both sides of the Atlantic.
- 'Privacy Protection in the Financial Sector: Fintech Innovations and Traditional Banking' ended with the announcement of a large-scale innovative initiative called Regtech Sandbox, which is due to be

implemented next year. It should be noted that such an idea in the field of privacy and personal data has not yet been implemented in Europe.

- 'Cyber Security Insurance – Building upon GDPR Compliance' presented the possibilities of using insurance products in the field of cybersecurity as well as the difficulties in formulating such products.
- 'Outsourcing Data – Global Data Transfer and Cloud Services' – trends and threats in the implementation of global business initiatives were considered.

The topics of individual events in Sofia were as follows:

- 'Canaries in a coal mine? Data Protection Officers in the data mine!' presented by the data protection officer of Europol and his team.
- 'Drones: Ethics of a PlayStation Mentality' presented by LIBRe Foundation and United Drone Community.
- 'The First Five Months of the GDPR' presented from the point of view of international private sector organisations and of a national supervisory authority.
- 'GDPR – Questions and Answers' (regarding the national implementation of the General Data Protection Regulation) presented by the host data protection supervisor, a state institution and a non-governmental organisation.
- 'EU-funded projects as a partnership and data protection instrument' presented by the Bulgarian national supervisory authority.

Within the framework of the Sofia programme, the participants had the opportunity to visit and get acquainted with the activities of the Laboratory of Artificial Intelligence and CAD Systems and the Cyber Security Laboratory on the territory of Sofia Tech Park.

Discussions from Brussels were transmitted to Sofia through an all-day videoconferencing between the two venues of the event. All participants, regardless of their location, had the opportunity to participate fully in the discussions through the Mobile Application of the Conference. In this way, the participants from Sofia followed open sessions in Brussels with a central topic ethics in the digital world. During the two seminar days, the participants heard many welcome addresses and video addresses. Within 5 sessions, an interactive, multidisciplinary and comprehensive debate took place and reflected the digital revolution, its impact on society and how digital ethics could help maintain dignity and respect in technology-driven life.

4. Participation of the CPDP in the activities of the Bulgarian presidency of the Council of the EU during the first half of 2018

Between January and June 2018, the Republic of Bulgaria had the rotating presidency of the Council of the European Union for the first time. The Bulgarian presidency was part of a trio together with Estonia and Austria.

CPDP was actively involved in the implementation of the priorities and objectives of the Presidency and was fully committed to their implementation in the area of personal data protection.

Dossiers and Achieved Results

Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions (modernised Regulation No 45/2001)

The proposal for a regulation updates and modernises the provisions of the currently effective Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data in order to bring them in line with the new EU legal framework in the field of personal data protection adopted in April 2016.

Despite the initially strong opposition from most delegations, including Germany, France, the UK, etc., the CPDP's negotiating team managed to change the positions of all the participants in the legislative process, including of the 28 Member States in the Council, the political groups in the EP and the European Commission, and on 23 May 2018 they **unanimously supported** the final compromise on the regulation proposed and negotiated by the Bulgarian Presidency. The key elements of the compromise were as follows:

- the modernised Regulation 45/2001 includes a separate chapter with common rules on the protection of data subjects' rights in the processing of operational personal data by Union agencies in the field of justice and home affairs. At the same time, the legal acts whereby the agencies in question are established can provide for special rules that deviate from the general rules where this is necessary and justified (*lex specialis derogat legi generali*);
- the provisions of the new chapter on operational personal data are identical or as close as possible to the rules laid down in Directive 2016/680 (the Police Directive). This ensures harmonization of the rules applicable to national law enforcement agencies and EU agencies;
- the provisions regarding operational personal data will be implemented immediately for Eurojust and Frontex, and for Europol and the European Public Prosecutor's Office – after 4 years and following a preliminary analysis to be carried out by the Commission.

Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust)

Regardless of the fact that the proposal for a Eurojust Regulation was considered in another working group by a team of the Ministry of Justice, the EP bound it to finding a solution to the issue of operational personal data (the so-called legislative package). For this reason, the successful conclusion by the CPDP of the negotiations on the modernised Regulation 45/2001 became the most important factor for reaching an agreement on the draft Eurojust Regulation on 19 June 2018.

Modernisation of Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data

The negotiations for the modernisation of Council of Europe Convention No 108 started in 2012. During the Bulgarian Presidency, the dossier became a priority political issue in the field of personal data protection, as the document is the only international legal instrument in this area. The modernisation of the Convention in fact encourages and promotes globally the introduction of the high EU standards for the protection of privacy and personal data.

Despite the serious political and diplomatic obstacles, at the last possible moment the EC managed to reach a compromise on the disputed texts with the Russian Federation and thus paved the way for the signing of the Protocol amending Convention No 108.

The final open issue on the dossier, to which the CPDP team had to find an urgent solution, was the clauses concerning the entry into force. The Council of Europe's legal committee proposed that the amendment should enter into force through classical ratification by all parties, while the EU, through the EC, insisted on a more ambitious and quick approach. The EU Member States were initially divided and supported three different options. Nevertheless, the Bulgarian Presidency managed to negotiate a **unified position of all Member States** on a compromise proposal for the entry into force of the Amending Protocol, which allowed the modernised Convention No 108 to be approved and adopted by the Committee of Ministers of the Council of Europe on 18 May 2018.

Other topics

During the Presidency, the CPDP team also organised discussions in DAPIX on other topical issues in the field of personal data protection, including ICANN, personal data protection clauses in EU trade agreements, the Japan Adequacy Decision and others.

CABO VERDE / CAP VERT

Activités menées depuis juin 2018

La CNPD, outre les activités de routine, telles que les enregistrements et les autorisations de traitement de données, a émis des avis, a engagé des procédures contre-administratives et a déclenché plusieurs activités de sensibilisation en publiant des brochures de support.

La CNPD a organisé et participé à plusieurs conférences et ateliers, dont la plupart visaient à sensibiliser les jeunes et les adolescents aux risques liés à l'utilisation des technologies numériques associées à Internet et aux plateformes de réseaux sociaux en ligne. Dans ce cas particulier, diverses activités ont eu lieu dans les écoles secondaires et les universités.

La CNPD a reçu dans ses locaux des citoyens, des entités publiques et privées, notamment les élus locaux de la capitale, pour des séances de clarification de la protection des données.

Il a également tenu des réunions avec l'Association nationale des municipalités du Cap-Vert et des associations professionnelles en vue de se conformer à la loi sur la protection des données à caractère personnel.

Dans le cadre du dialogue institutionnel avec le gouvernement, le ministre chargé des affaires parlementaires et la présidence du Conseil des ministres a visité la CNPD afin de s'informer de son fonctionnement et de l'articulation entre la CNPD et les différentes instances de l'administration publique.

En septembre 2018, la CNPD a tenu une séance de travail avec un conseiller de l'Union internationale des télécommunications (UIT) afin de partager leur expérience en matière de création de l'autorité de protection des données de la Jamaïque.

En octobre 2018, la CNPD a participé à la réunion annuelle et à la 12e assemblée générale de l’Association francophone des autorités de protection des données personnelles (AFAPDP), qui ont eu lieu les 18 et 19 octobre 2018 à Paris, en France. À cette occasion, elle a été admise en tant que membre de l'AFAPDP.

Elle a ensuite participé à la 40e Conférence internationale des commissaires de la protection des données et de la vie privée, qui s'est déroulée à Bruxelles, en Belgique, du 22 au 26 octobre 2018, sous le slogan: DEBATTRE L'ÉTHIQUE: Dignité et respect dans Data Driven Live. La CNPD était présente.

La CNPD a participé à la XVIe réunion du réseau ibéro-américain de protection des données, dont elle est membre observateur, qui s'est déroulée au Costa Rica les 28, 29 et 30 novembre.

La CNPD était représentée au Sommet annuel sur la protection des données en Afrique sur le thème "Briser les nouvelles frontières", qui s'est tenu à Maurice du 19 au 23 novembre 2018.

Pour marquer la date de la protection des données, le 28 janvier, la Commission nationale pour la protection des données (CNPD) a reçu à son siège de Praia, des étudiants de l'école technique Gran Duque Henri, située à Assomada, dans l'île de Santiago.

En commémoration de son 4e anniversaire, la CNPD a organisé le 23 avril une conférence sous le slogan "Données personnelles, réseaux sociaux en ligne et démocratie".

C’était le moment de discuter de questions telles que le droit à la vie privée et la protection des données dans l’environnement numérique, les problèmes de protection des données des électeurs, les réseaux

sociaux en ligne et les défis pour la protection des données et les mécanismes de coopération internationale.

La Conférence a été ouverte par Son Excellence le Président de l'Assemblée nationale du Cap-Vert. Un des panneaux a été présenté par Mme Sophie Kwasny, Chef du Groupe de la protection des données du Conseil de l'Europe.

Plus de 130 participants étaient présents, parmi lesquels des membres du corps diplomatique, des députés, des responsables nationaux et locaux, des magistrats, des universitaires et des étudiants.

Au cours de son séjour au Cap-Vert, Mme Sophie Kwasny a rencontré les membres du CNPD le 22 avril. Cette réunion a porté sur des questions liées au fonctionnement de la CNPD, à ses relations avec d'autres autorités et organisations internationales et à la mobilisation de partenariats.

Le chef de l'unité "Protection des données" du Conseil de l'Europe a également été reçu en audience par SE le Président de l'Assemblée nationale du Cap-Vert. Les deux ont convergé sur l'importance de la protection des données à caractère personnel à l'heure actuelle et de l'octroi de plus de moyens à la CNPD.

Dans son rapport sur les activités pour 2018, la CNPD a suggéré à l'Assemblée nationale du Cap-Vert des mesures législatives concernant:

• Le Régime juridique général pour la protection des données et son alignement sur la 108ème Convention modernisée;

• La Loi réglementant l'installation et l'utilisation de systèmes de vidéosurveillance;

• Le Régime juridique pour le traitement de données dans le secteur des communications;

• La Législation sur l'utilisation d'aéronefs sans équipage, normalement appelée drones.

• L' adhésion du Cap-Vert à la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel.

Commission Nationale pour la Protection des Données

Praia, le 5 juin 2019

CROATIA / CROATIE

This reporting period is specific due to the fact that it is marked by the full application of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation (EU L119)) on 25 May 2018 and the adoption of the Act on the Implementation of the General Data Protection Regulation (OG 42/18)*.*

According to Article 51 of the General Data Protection Regulation, the Croatian Personal Data Protection Agency is the supervisory authority responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union*, and as part of its tasks and powers, it acts daily to raise awareness of the importance of personal data protection.*

Act on the Implementation of the General Data Protection Regulation (OG 42/18)*, in Article 14, prescribes that the central state administration bodies and other state bodies are obliged to submit to the Agency drafts of the legislative proposals and proposals of other regulations regulating personal data processing issues for the purpose of giving expert opinions regarding the area of personal data protection and the Agency acts in accordance with the above.*

In the period of full application of the General Data Protection Regulation of 25 May 2018, comparing the dynamics of the receiving of cases in the previous reporting periods, there has been a significant increase in the number of cases received in relation to the reporting period so far, and the cause is the application of the General Data Protection Regulation which, from 25 May 2018, is directly applicable in all EU Member States. We are providing you with the statistics about received inquiries, claims for protection and supervisory and educational activities in the reporting period:

Inquiries	*2896*
Administrative procedures	*144 (60 closed)*
Requests for determination of a violation of a right	*1470*
Educational activities	*60*
Supervisory activities	*214*
Number of draft regulations submitted for the purpose of providing expert opinion pursuant to article 14 of Act on the Implementation of the General Data Protection Regulation	*48*

The Croatian Personal Data Protection Agency has intensively conducted educational activities that are primarily related to the advisory role of the Agency as the competent and supervisory body. In the reported period, the Agency realized a total of 60 major activities of consultancy, education, conferences, workshops, lectures, round tables and occasionally organized events. The Agency has carried out a large number of education and information activities of all stakeholders, enabling the public to obtain as much information as possible on the new legislative framework in the area of personal data protection, with an emphasis on the principles, requirements, obligations and provisions laid down by the GDPR.

Accordingly, in this reporting period, the information and educational content of the Agency was available to the public through brochures and printed material, textual and pictorial announcements on the official

website of the Agency (with the possibility of downloading), presentations, mobile applications, publication in print and digital media, TV and radio reports, and all other materials that ensure the availability of information,

Aware of the intense need for a very specific knowledge, necessarily needed, and especially after the adoption of the new legislative framework of the European Union and the Republic of Croatia, in the second half of 2018 an expert recruitment plan has been implemented, mainly for the area of law and information security and information technology. In 2018, in comparison to 2017, the number of lawyers in the Agency's work organization was 11 (in 2017) to 21 (in 2018), which represents an increase in the number of 91% with legal knowledge. The percentage share of employees with specific information, IT and technical knowledge has increased from 4 to 6 which means by 50 percent compared to the previous year. Raising the qualification level of employees compared to the previous years was primarily influenced by the employment of highly qualified new employees. Accordingly, in the educational structure of the Agency in 2018, 82 percent of employees have an academic degree of education - high qualifications.

This reporting period, the Agency concludes with a total of forty employees who, because of their specialization, represent the Agency's greatest strength and source of knowledge in the field of personal data protection in the Republic of Croatia.

Consequently, the continuous focus of the Agency in its work and operations is manifested mainly through the creation of presumptions for the effective and legally harmonized protection of personal data as well as the supervision of the processing of personal data of Croatian citizens, thus contributing to the realization of the fundamental rights of the European Union and the Constitution of the Republic of Croatia, of every individual on the protection of personal 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 however with a certain delay.

The Act No. 110/2019 Coll., on processing of personal data and the Act No. 111/2019 Coll., amending some acts in relation to the adoption of the act on processing of personal data became effective as late as of 24 April 2019.

ESTONIA / ESTONIE

Major developments in the data protection field in Estonia since June 2018

1. Legislation

The year of 2018 was the year of data protection reform. Estonian implementing legislation (Personal Data Protection Act) for the General Data Protection Regulation took some time and it was enacted in January 2019. Additional implementing act for the Personal Data Protection Act was enacted in March 2019.

Public Information Act, transposing the Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies, mandates Estonian Data Protection Inspectorate as a supervisory authority.

2. Relevant cases

2.1 Estonia have new Cybersecurity Strategy for 2019-2022

The Ministry of Economic Affairs and Communications has launched new Cybersecurity Strategy for the years 2019-2022. It is Estonia's third national cybersecurity strategy document and it defines the long-term vision, objectives, priority action areas, roles and tasks for the domain, being the basis for activity planning and resource allocation.

The aim of the strategy is to agree on and create conditions for the implementation of a comprehensive, systematic and inclusive sectoral policy.
The Cybersecurity Strategy was prepared in a coherent process with Estonia's Digital Agenda 2020. The experiences has brought an understanding that in a successful digital society, developing information society and ensuring cybersecurity must be a strategic whole. The role of cybersecurity in the information society is to ensure conditions for efficient and secure use of opportunities offered by ICTs.

2.2. *Renewed open data portal*

Pursuant to the Public Information Act, all holders of information (e.g. public sector authorities, municipalities) have to publish for the public use information which is not restricted by law or pursuant to the procedure established by law, in the form of open data. Supervisory authority is Estonian DPA. The general coordinator of the open data in Estonia is Ministry of Economic Affairs and Communications. They manage open data portal opendata.riik.ee. The purpose of public data disclosure is to ensure democratic governance, transparency and the ability to monitor the performance of public tasks, but also to value and implement data. Public data is allowed and even welcomed for business purposes. In addition, the collection of open data on a single portal facilitates the deployment of artificial intelligence solutions that can also implement these data in their work.

2.3. *Updated personal data processing guideline*

Estonian Data Protection Inspectorate has updated general data processing guideline for controllers and processors. Based on the European Data Protection Board Opinion 6/2018, renewed guideline has an extra section, explaining the criteria, when the data protection impact assessment is mandatory for cross border data processing. The guideline is available here (in Estonian).

FINLAND / FINLANDE

Overall reform of the data protection legislation

Finnish Parliament adopted on 13 November 2018 a new Data Protection Act (1050/2018) to supplement the provisions of 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 (GDPR). The Data Protection Act entered into force on 1 January 2019, repealing the Personal Data Act (523/1999) and the Act on the Data Protection Board and Data Protection Ombudsman (389/1994) were repealed. The Act provides for the national supervisory authority and the procedure for imposing administrative fines as required by the Regulation. The Act also supplements and adapts certain provisions of the Regulation.

The Data Protection Ombudsman is competent to impose a conditional fine in certain situations provided by law. A collegium of the Data Ombudsman and the Deputy Data Ombudsmen may impose administrative fines provided for in the GDPR, for violations of the data protection legislation. Instead of administrative fines, however, public authorities and public law entities are subject to criminal law sanctions.

The Data Protection Act applies within the scope of application of Article 2 of the GDPR. The Act and the GDPR also apply, with the exception of Article 56 and Chapter VII of the GDPR, to the processing of personal data in the course of activities referred to in points (a) and (b) of Article 2(2), unless otherwise provided by law.

At the same time with the Data Protection Act, a new Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018) was adopted. This Act, which also entered into force on 1 January 2019, transposes the provisions of Directive (EU) 2016/680 of the European Parliament and of the Council 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. The scope of application of the Act is, however, wider than that of the Directive, covering to a large extent even the processing of personal data for the purposes of national security by specific authorities referred to in the Act.

The Act 1054/2019 is generally applicable to the processing of personal data by the competent authorities, but may be supplemented by legislation applicable to specific authorities. Certain legislative acts in the law enforcement sector have recently undergone an overall revision, with entry into force on 1 June 2019. Minor amendments were earlier made to the Act on the processing of personal data by the Prison Administration, with entry into force on 1 January 2019. The duties of the Data Protection Ombudsman also cover the supervision of the processing of personal data in the law enforcement and criminal law sectors and in the field of national security.

The reform also gave birth to a new profession, the Data Protection Officer. The new Officers and their assistance to data subjects and controllers are a positive development.

In connection with the legislative work in Parliament, the work of the Parliamentary Constitutional Law Committee was particularly noteworthy. The Committee redefined its policies on enactments governing the protection of personal data in relation to the directly applicable GDPR.

Data Protection Ombudsman

The Data Protection Act maintained the Data Protection Ombudsman as the national supervisory authority. The Data Protection Ombudsman's powers of investigation and access to information were revised and extended in accordance with the EU legislation. The Office of the Data Protection Ombudsman has been reorganised on the basis of the Data Protection Act. The Data Ombudsman is assisted by two Deputy Data Protection Ombudsmen and by a number of other personnel. The Act also provides for a five-member expert board.

The Data Protection Ombudsman has faced an increased amount of work in the past year. The Office of the Data Protection Ombudsman registered 9,617 cases instituted in 2018, while the corresponding number in the previous year was 3,957. As a result of the reform of legislation on the processing of personal data and related legislative acts, the Data Protection Ombudsman was heard by Parliament 93 times in 2018. The Data Protection Ombudsman has also actively participated in the work of the European Data Protection Board (EDPB), which began operations in May 2018.

The Office of the Data Protection Ombudsman is seeking to adapt its operations to the data protection reform by improving its competence management. Some new resources have been allocated to the Office of the Data Protection Ombudsman.

Due to the enactment of new intelligence legislation, an independent Office of the Intelligence Ombudsman will be established parallel to the Office of the Data Protection Ombudsman.

The Data Protection Ombudsman has published the annual report on its activities in 2018. The report is available in English at: https://tietosuoja.fi/en/annual-report-2018

GEORGIA / GEORGIE

Office of the Personal Data
Protection Inspector

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD

June 2018 – June 2019

GEORGIA

INCREASED PUBLIC INTEREST TOWARDS PRIVACY

Georgia is witnessing increased public interest towards privacy. The level of awareness on data protection issues in the private sector, large and medium sized business, as well as the interest in prior consultations with the Inspector's Office have significantly increased. An essential portion of more than 6100 consultations (25% more compare to the previous year) in 2018 was provided to the citizens.

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, citizen's complaints and consultations

The tendency of increasing citizen's complaints and conducted inspections remains unchanged for the sixth year in a row. In comparison to 2017, in 2018 the number of citizen's referrals was increased with 60% and the number of conducted inspections – with 30%. Importantly, against the increase in the number of citizens' complaints and conducted inspections, for the first time during the last 6 years a decrease in the number of violations and fines was observed.

In the reporting period the Office studied 115 data processing operations in public sector, including various ministries, courts, election administration, local self-governments. 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 2018, the Office of the Inspector studied and reviewed 355 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 6100 consultations have been delivered in

2018 that marked a 25% increase compare to 2017. From this overall number of consultations, up to 900 were delivered to public bodies, more than 2,100 − to private organizations and more than 4,000 − 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 organizations and the representatives of the media and civil society. Throughout 2018 1200 representatives from public and private sectors were given an opportunity to gain and enhance knowledge on personal data protection issues.

Several important developments have taken place in order to raise awareness of the population:

- With the support of the EU and UNDP a new web-page was developed and adapted to the needs of persons with disabilities;
- A new case management system was introduced that after the user's registration enables any type of communication with the Inspector's Office in a single online space;
- A guidebook on new EU regulation was drafted, translated and is now available on the Inspector's web-page;
- Recommendations for healthcare institutions, higher educational institutions and commercial banks were prepared and presented to the public.

International cooperation

The Inspector's Office is still actively involved in the fulfillment of Georgia's international obligations, including the implementation of EU-Georgia Association Agenda. The Inspector was actively participating in international platforms and conferences, hosting delegations from different countries and sharing Georgian experience.

In May 2019, the Office hosted 29th edition of the Spring Conference of European Data Protection Authorities. The conference was attended by more than 70 representatives of data protection authorities, European institutions and international organizations.

LEGISLATIVE ACTIVITY

In light of the EU data protection reform and modernization of Convention 108, the Office finalized new draft of the Personal Data Protection Act which will replace the current law. The Inspector's Office conducted a comprehensive study of the EU GDPR and the existing Georgian legislation. New law will contribute to the harmonization of Georgian legislation with the European standards, fulfillment of the obligations laid down in the Association Agreement and improvement of the standards of personal data protection in the country.

The draft law is already initiated in the parliament for further legislative procedures.

Other than this the Office was actively engaged in the law-making process and cooperated with legislative and executive government bodies. The employees of the Office participated in working meetings, committee discussions and other formats. in order to ensure compliance with data protection legislation the office submitted opinions regarding 40 legislative initiatives and studied over 100 draft laws and bylaws regulating various legal areas. The mentioned draft documents were related to educational,

financial, audit, archiving, electoral and other activities; healthcare, public security, electronic communications, children, persons with disabilities and other issues. The Office was also involved in the work on the international treaties with the Euro Just and Europol.

The Office is actively lobbying the process of signature of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Number of meetings with relevant state agencies have taken place with the aim to accelerate the process.

GERMANY / ALLEMAGNE

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

- The new Federal Data Protection Act (covering both Regulation (EU) 2016/679 - General Data Protection Regulation and Directive (EU) 2016/680 and some amendments to the laws of the federal intelligence agencies) was adopted by parliament in May 2017 and published in the official journal on 30 June 2017. The Act entered into force on 25 May 2018. The new Federal Data Protection Act can be found at:
  https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1519203215836, or
  https://germanlawarchive.iuscomp.org/?p=712

- The Federal cabinet approved a draft on 154 amendments to sector specific legislation on 5 September 2018. The draft can be found at:
  https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/dsanpug.pdf;jsessionid=A250D36F41A80F0321F354195365D87D.2_cid373?__blob=publicationFile&v=2

  A first (smaller) part of amendments to some federal legal acts in the tax and social security area was adopted in July 2017 and published in the official journal on July 17; it entered into force on 25 May 2018.

- The Federal cabinet approved also a draft on amendments to the German Code of Criminal Procedure and a number of amendments to justice related legislation on 22 August 2018. The draft can be found at:
  www.bmjv.bund.de/stpo_datenschutz

- The 16 Länder adopted their general data protection acts. An overview with links to the texts can be found at:
  https://www.esv.info/aktuell/umsetzung-der-dsgvo-neues-aus-bayern-und-nordrhein-westfalen/id/93637/meldung.html

  The Länder are currently working on the adaption of their sector specific legislation.

GREECE/ GRECE

We inform you that currently Greece is expected to proceed with the entering into force of the implementation law of the EU Directive 2016/679 regarding the Protection of individuals with regards to the processing of their personal data (GDPR) and of the EU Directive 2016/680 regarding the processing of personal data by supervisory authorities and transborder data flows. The ratification law has been on public consultation until 5th of March 2019. The aforementioned implementation law will cover all provisions and requirements of the Convention 108, its ratification remaining only to be concluded.

HUNGARY/ HONGRIE

Major developments in the data protection field in Hungary and the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter "NAIH") since the General Data Protection Regulation (hereinafter "GDPR") has entered into force

I. Legislation

During June and July, 2018 the Hungarian Parliament adopted two pieces of legislation aimed at implementing the GDPR and transposing the Law Enforcement Directive (hereinafter "LED") into the Hungarian legal system. Act XIII of 2018 (entering into force on the 30th of June) empowered the National Authority for Data Protection and Freedom of Information to exercise the tasks and powers conferred to the supervisory authorities by the provisions of the GDPR and the LED. Whereas by Act XVIII of 2018 the Hungarian legislator paved the way to the direct application of the GDPR, adopted the rules necessary to comply with the LED, and regulated data processing activities (national security, defence) that fall outside the scope of Union law.

In March, 2019 a bill comprising amendments of a number of sectorial laws was submitted to the Parliament by the Government. The bill was adopted and the amendments entered into force in April and thus provide for GDPR-compatible rules applicable to the processing of personal data in the course of various activities (e.g. employment, public health, public services etc.). However, certain sectorial laws (e.g. direct marketing in the online environment) are not covered by the amendments and are expected to be reviewed by the lawmaker as soon as possible.

2. New tasks

The entry into force of the GDPR in 2016 and its subsequent application since May 25, 2018, have not only brought major changes in the lives of data controllers and processors, but also in the organizational structure and tasks of the NAIH.

Department of Data Protection

In accordance with the GDPR, the amended Hungarian legislation introduced a **new type of data protection authority procedure**, to be launched on the application of the data subject ("client"). The basis of this procedure is Article 77 of GDPR and it aims at ensuring the right to lodge a complaint with a supervisory authority.

Besides, a substantial change concerning the tasks of the NAIH appeared due to the **formalized cooperation with the data protection authorities of the European Union**.

The progressive increase of the requests for information and interpretation of the provisions introduced by the data protection reform shows the substantial uncertainty with regard to the application of the GDPR. However, the room for manoeuvre for the NAIH is rather limited for responding such requests because of the fact that the European Data Protection Board is solely entitled to interpret authentically and abstractly the GDPR in order to ensure the uniform application its provisions.

Department for Regulative Issues and Secret Surveillance

The control of gathering intelligence regulation and everyday practise is among one of the main priorities of the Hungarian Data Protection Authority. On the 1st July 2018 the new law of criminal process (Act XC of 2017) entered into force, which meant a major change in the field of the secret information gathering. NAIH welcomes that the new regulation defines the concept of 'covered tools' with greater accuracy than it has done before and it uses tools and methods in a newly designed system.

The Ministry of Interior had been working since 2017 on a project called 'Dragonfly' and in 2018 the project has reached a point when the Ministry invited NAIH to discuss its details and to give an opinion on the draft piece of legislation. As it turned out, the project is about storing videos and photos of 35 000 cameras working at various places in Hungary, like streets, public places, public transport vehicles. This amount of data is going to be stored in a governmental datacenter. During the discussion NAIH managed to achieve some progress regarding data protection during the drafting process, the bill was adopted by the Parliament in December 2018. The project is going to be completed in the next few years.

3. New tasks - New organizational structure

Cabinet of the Vice-President

The **Cabinet of the Vice-President** of the NAIH (hereinafter "CoVP") formed as a result of organizational changes, plays a prominent role in coordinating international cooperation and consistency mechanisms as professional organizational unit. It also contributes to the tasks of the Vice-President of the Authority concerning the European Data Protection Board (hereinafter "the Board") and the work of expert subgroups consisting of national experts of the data protection authorities (N.B.: the Authority is represented in each expert subgroup). On behalf of the NAIH, the staff of the CoVP manages the main administration of cases uploaded to the IMI (Internal Market Information System). Finally, the CoVP carries out tasks related to and coordinates the representation of the NAIH on the monthly plenary sessions of the Board. The agenda of the plenary sessions is discussed in and approved by the GDPR Working Group within the NAIH, in which the CoVP plays an active role and which is presided by the Vice-President of the Authority.

Department of Authorization and Data Breach Notification

The Hungarian Data Protection Authority received several data breach notifications from various data controllers since 25th May 2018. The NAIH launches administrative audits according to the Code of General Administrative Procedure regarding all data breach notifications. NAIH launches official administrative control procedure if it detects the infringement of the GDPR during the administrative audit. The NAIH received more than 400 data breach notifications since the applicability of the GDPR, but issued an administrative fine in only three cases.
One of the three cases is summed up in the following:
the NAIH received a notification of public interest regarding a webpage http://web.dkp.hu operated by the Democratic Coalition, in which the NAIH was informed that the database found on this webpage - with all the users' personal data (e-mail addresses, names and the encrypted passwords) - is openly accessible, presumably by way of an unknown hacker accessing to the vulnerable webpage then uploading the data to https://defuse.ca6b6DIOCGRER7ZE1qVeDyVKpg1.
With respect to Article 9 (1) and Article 33 (1) of the GDPR and the Hungarian Privacy Act Section 60 (1) the NAIH launched an administrative control procedure, which led to a data protection administrative procedure in November 2018.

Aggravating circumstances in the case were that the concerned data are special categories of personal data revealing political opinions; the controller used an out-of-date encryption technology; the controller had not notified the personal data breach to the SA, although it had been aware of it, and did not communicate the breach to the 6000 data subjects. It was considered an attenuating circumstance that the controller implemented appropriate measures to eliminate the cause responsible for the data breach. The NAIH issued an administrative fine of 11.000.000 HUF (approx. 35.000 EUR) in the case.

Regarding data protection impact assessments, no prior consultations (Article 36 of the GDPR) has been initiated with the NAIH by data controllers yet, but a free, open-source impact assessment software is available on the authority's website to assist controllers during this procedure. The software can be downloaded via the following link: http://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html.

According to the Hungarian Privacy Act Section 64/C the NAIH shall also conduct a procedure for the authorisation of data processing if an application
a) for the approval of the draft, extension or amendment of the codes of conduct referred to in Article 40;
b) for the authorisation of the monitoring activity referred to in Article 41;
c) for the approval of the certification criteria referred to in Article 42 (5);
d) for the authorisation of the contractual clauses referred to in Article 46 (3) (a);
e) for the authorisation of the provisions referred to in Article 46 (3) (b);
f) for the approval of the binding corporate rules referred to in Article 47
of the General Data Protection Regulation is submitted.

An administrative service fee, as determined in a ministerial decree, shall be paid for the authorization procedure. The time limit for the procedures is 180 days for applications referred to in points a) to c) and f), and 90 days for applications referred to points d) and e). In its decision, NAIH approves of /authorises or dismisses the application.

As for now, no authorization procedures has been initiated at the Authority by data controllers since the entry into force of the GDPR.

ICELAND/ ISLANDE

Information on Major Developments in the Data Protection Field Since June 2018

The Icelandic Data Protection Authority
At the moment, 17 people work at the Icelandic Data Protection Authority, including 8 lawyers, 2 information security experts, 2 archiving employees, 4 office managers and the Data Protection Commissioner, Ms Helga Þórisdóttir. The chair of the DPA's board of directors is Ms Björg Thorarensen.

On January 1st 2019, the DPA's annual budget was increased from 205,8 million ISK (Icelandic kronas) to 300,8 million ISK, due to a heavy workload at the authority. In addition, the DPA's funds will be gradually increased every year for the next three years, according to the government budgetary plan.

The New Act on Data Protection and the Processing of personal data
On 15 July 2018, a new Act on Data Protection and the Processing of Personal Data, No. 90/2018, entered into force. The act substitutes the Act no. 77/2000 on the Protection of Privacy as regards the Processing of Personal Data.

The Act implements into Icelandic law the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Public Awareness
In order to raise data protection awareness, the Icelandic DPA has organized 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:

A special promotional campaign
A promotional campaign was held in October and November 2018 with open meetings in 9 locations across the country. In parallel, brochures were prepared with a summary of information for small and medium size companies, as well as the general public. These brochures are available at the DPA's website, www.personuvernd.is.

Published material
The DPA has published over twenty guidelines and brochures on the DPA's website in order to raise awareness about data protection amongst companies, public organizations,, individuals and others who work with personal data. To name a few, these guidelines include a list regarding the processing operations subject to the requirement of a data protection impact assessment, recommendation on the use of social media in schools, guidelines on security breaches, guidelines for processors, educational material for DPO's and information for companies in Iceland because of Brexit.

Media Coverage
Data protection related matters continue to be extremely popular with the Icelandic media. On numerous occasions, the Data Protection Commissioner has been interviewed regarding data protection related subjects in newspapers, radio and televison.

Other Actions
The DPA set up a special service desk for companies that request guidance regarding the implementation of the new Data Protection Act. Then the DPA has given lectures and presentations on GDPR and other data protection related matters on many occasions in the past year.

Statistical Data

According to statistical data, during 2018 the DPA received a total of 2414 cases, including 99 complaints, 1034 inquires, 13 inspections and 296 cases related to scientific research within the health sector.

Annual Report of the DPA
The Annual Report of the Data Protection Authority, which provides further information in relation to the activities of the DPA during 2018, will be available soon at the DPA‘s website.

Other
The Annex to Convention no. 108, which seeks to update the Convention in the light of technological development and to strengthen the validity of the Convention in its Member states, which had formerly been approved by the T-PD, was signed on behalf of Iceland on November 21st 2018.

IRELAND / IRLANDE

Report from Ireland on Major Developments

(June 2019)

Digital Summit 2019

The Department of the Taoiseach (Prime Minister) is currently planning the Digital Summit 2019, scheduled to take place on 20 September 2019. This event is a follow up to last year's very successful Data Summit 2018, which involved many internationally recognised speakers and attracted a national and international audience of approximately 400 people from a range of disciplines. The Data Summit 2018 highlighted many of the important initiatives and developments that have originated from the EU, such as the implications of the General Data Protection Regulation and initiatives relating to Artificial Intelligence. The Summit was designed to underline the Government's commitment to exploring policies that maximise the potential of data driven technologies for the good of our society and economy.

The Digital Summit 2019 seeks to continue the dialogue on data and digital related developments and their ever-expanding role in modern society established last year. The Summit is rebranded to address the digital transformation taking place nationally and internationally. Topics to be discussed at the Summit include: artificial intelligence and its potential impact on how we live and work, the future of data and privacy, and digital technology and well-being. The Digital Summit 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 digital in our society.

Proposed National Digital Strategy

A Framework for Developing the new National Digital Strategy, was approved by the Irish Government in July 2018. This reflected preliminary stakeholder consultations with civic society, business representatives, education providers and academia.

A wider public consultation exercise, to allow citizens to influence the development of the Strategy, then took place in the final quarter of 2018. Over 300 responses were received. In parallel, wide ranging consultations with stakeholders and sectoral experts to inform development of the Strategy took place.

The drafting of the Strategy continues to progress to take account of the broad spectrum of inputs that have been garnered in this time. It will set out Ireland's vision and ambition across thematic areas, including

- digital infrastructure and security
- trust and well-being
- effective use of digital by citizens, communities, enterprise and government, and
- the digital economy's impact on the labour market.

Importantly, it will also position Ireland internationally and within the European Union, where we are active promoters of the digital Single Market. It is anticipated that it will emphasise issues such as connectivity, cybersecurity, greater use of open data, proactive regulation, public trust in digital, improved online public services, greater understanding of digital well-being, digital skills, and the digital intensity of SMEs.

Introduction

The 25th May 2019 marks the one year anniversary of the introduction of the General Data Protection Regulation across the EU, as well as the one year anniversary of the introduction of the Data Protection Act 2018 in Ireland, and the reestablishment of the office of the Data Protection Commissioner as the Data Protection Commission under the new regulatory framework.

The 2019 funding allocation for the DPC is €15.2 million which represents a 30% increase on the 2018 allocation. It is intended to recruit approximately 40 additional staff in 2019 bringing the DPC's total staff to approximately 180.

12 months on from GDPR: statistics

The 12 month period since the introduction of the new statutory framework has seen a remarkable rise in the number of complaints and queries to the Data Protection Commission (DPC), demonstrating a new level of awareness on the part of individuals of their rights to the protection of personal data. The response from data controllers has been just as strong, with high numbers of Data Protection Officer notifications and data breach notifications to the DPC.

Key figures from 25 May 2018 – 24 May 2019:

- 6,624 complaints to the DPC
- 5,818 data breach notifications to the DPC
- Approx. 48,000 queries to the DPC
- 1,206 Data Protection Officer notifications to the DPC

Guidance, awareness, and consultation

The DPC has engaged extensively in promoting awareness of the DPC through outreach and engagement, formal consultations, and formal guidance publications.

Key figures since 25 May 2018:

- The Commissioner and her staff have spoken, presented, or otherwise contributed at events on over 183 occasions.
- 15 formal guidance documents and 6 blog posts published.
- DPC website relaunched and website guidance fully updated for new statutory framework.
- 1,543 consultations with data controllers/processors.
- Approx. 4.4 million social media impressions.
- Publication of final Annual Report of the Data Protection Commissioner covering the period 1 January to 24 May 2018, and publication of first Annual Report of the Data Protection Commission covering the period from 25 May to 31 December 2018. The reports are available on the DPC's website: www.dataprotection.ie.

Enforcement

The DPC has opened 55 formal statutory investigations since the 25 May 2018. These include:

- 35 non cross-border investigations, all of which are into public bodies
- 20 cross-border investigations, all of which are into multinational technology companies

A number of these investigations are at an advanced stage.

Children's Consultation
The DPC has engaged in a landmark consultation on issues relating to the processing of children's personal data and the rights of children as data subjects under the GDPR.

.

The consultation encompassed two streams. Stream one was aimed at adults and interested parties were invited to make written submissions to the DPC. Stream two was aimed directly at children and young people. The DPC piloted an in-classroom consultation with the support of the Office of the Children's Ombudsman, and subsequently developed a pack of consultation materials including a specially created lesson plan on personal data and data protection rights in the context of social media. Invitations to take part in the consultation using these materials were sent to all schools and Youthreach centres.

DPO Network
The DPC intends to establish a Data Protection Officer Network in 2019, to facilitate the sharing of good practice and lessons learned through peer-to-peer DPO support. In advance of this initiative, the DPC has sought the views of DPOs and submissions received are currently being processed.

Regulatory Strategy
The Data Protection Commission is engaged in a significant project to develop its new Regulatory Strategy for the period 2020-2025. This process will be highly consultative and inclusive in terms of the stakeholder groups with whom the DPC engages, and that engagement will be ongoing throughout the development of the strategy.

European Data Protection Board
The DPC has engaged extensively with its counterpart DPAs at the European Data Protection Board.

- 548 'One Stop Shop' cases and requests since 25 May 2018.
- The DPC acted as lead rapporteur for the development of EDPB Guidelines on Codes of Conduct.
- The DPC has engaged extensively in EDPB sub-groups, task forces and working groups. The DPC has been represented on DPC groups covering the future of privacy, key provisions, cooperation, enforcement, technology, borders travel and law enforcement, international transfers, financial matters, eGovernment, fining, and social media.

ITALY/ ITALIE

Major developments in the data protection field

(Main source: Italian SA Annual Report 2018)

Data Protection Law

The Italian Data Protection Code was amended by the decree adapting the national legal system to the GDPR 2016/679 (Legislative Decree No. 101 of 10 August 2018). Accordingly, several of its provisions were amended or repealed and sections were added. The decree has made use of the margin of manoeuvre afforded by the GDPR to Member States as regards, in particular, processing activities based on legal obligations or for purposes in the public interest (Article 6(1), letters c) and e)); processing of biometric, genetic and health-related data (Article 9(4) and Article 36(5)); processing activities covered by Chapter IX of the GDPR (journalism, labour, research, archiving, etc.). As a result, several provisions of the 2003 Code were left in place as they were found not to be in conflict or overlap with the GDPR and to provide added value for the relevant stakeholders based on the implementing experience of the past 15 years.

With regard to the data protection rules in law enforcement, which were also part of the EU data protection reform package, legislative decree No. 51 of 18 May 2018 transposed directive 2016/680 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.

The past year marked a transition phase at supranational level as well. After the modernization process concerning Council of Europe's Convention 108/81 was completed, Italy signed the Amending Protocol to Convention on 5 March 2019.

Main activities of the Data Protection Authority

The applicability of the EU General Data Protection Regulation (25 May 2018) marked a veritable watershed moment in terms of the activities carried out by the Italian supervisory authority in 2018. Since that date, the SA focused on the new legal framework, in particular following entry into force of the national legislation enacted further to the GDPR – namely, legislative decree No. 101/2018, as mentioned above, which made substantial amendments to the so-called consolidated data protection code, i.e., legislative decree No. 196/2003. Special attention has been paid to a number of novelties introduced by the GDPR: enhanced cooperation with the other EU supervisory authorities; the amended rules applying to processing activities in the law enforcement sector; the various tools – such as the data protection impact assessment, the appointment of a data protection officer, the implementation of certification mechanisms, the accountability all data controllers are expected to ensure; and the more effective sanctions envisaged against this background.

As from 25 May 2018, the EU SAs also started cooperating under the terms of the GDPR to handle complaints and breaches related to cross-border processing activities. Coming more specifically to the activities carried out by the Italian SA after 25 May 2018 there was an increased work to bring the SA's operational mechanisms fully in line with the new legal framework. The so-called 'general authorisations' issued by the Garante applying to the processing of 'sensitive' data were revised pursuant to Section 21 of legislative decree No. 101/18, so that the provisions contained in those authorisations that were compatible with the GDPR could be identified by a decision dated 13 December 2018 – on which a public consultation was launched on 11 January 2019 via a notice published in Italy's official journal. Under the terms of Section 20(3) and (4) of the said legislative decree No. 101/2018, the SA assessed to what extent the provisions set out in some of the 'Codes of practice and conduct' attached to the data protection Code were compatible with the GDPR (in particular, the codes contained in Annexes A2, A3, and A4 to the Code). The compatible provisions were grouped into 'Rules of conduct' and attached to the amended data protection Code (Annex A). This exercise was also carried out with regard to the 'Code of practice applying to the processing of personal data in connection with journalistic activities', leading to the adoption of 'Rules of conduct applying to the processing of personal data in connection with journalistic activities' (Chapter 8). The multi-step revision process concerning other codes of practice and conduct (as

contained in Annexes A.5 and A.7 to the former data protection Code) was also started pursuant to Section 20(1) of legislative decree No. 101/2018.

Furthermore, a non-exhaustive list of cross-border processing activities subject to mandatory data protection impact assessment was also set out (see decision No. 467 of 11 October 2018), without prejudice to the guidance provided by the 'Article 29' Working Party in the 'Guidelines on data protection impact assessment' as last revised on 4 October 2017 and endorsed by the European Data Protection Board on 25 May 2018 (WP248, rev. 01).

Further clarification was provided concerning qualifications and activities of data protection officers, following the initiatives that had been implemented in 2017 – by way of ad-hoc meetings involving both public sector and private sector stakeholders and within the framework of wider-range initiatives.

Striking the right balance between transparency and personal data protection remains one of the topmost commitments for the Italian SA. This is shown by the many opinions rendered on FOIA-type access requests to Transparency and Anti-Corruption Officers as well as to Ombudspersons. Indeed, the SA itself received several FOIA-type access requests throughout 2018.

Reference should be made in this respect to the recent judgment by Italy's Constitutional Court (No. 20 of 23 January 2019), whereby Section 14(1-a) of legislative decree No. 33 of 14 March 2013 was found to be unconstitutional because in breach of reasonableness and equality principles. The said decree regulates FOIA-type access rights and the transparency, publicity, and disclosure obligations applying to public administrative bodies. The provisions at issue envisage that public administrative bodies must publish the information referred to in Section 14(1), letter f), of the decree with regard to all senior officials – i.e., a statement concerning rights in rem on immovable property and registered movable property, any stock or corporate interests held, and any positions covered as members of the board of directors or auditors for any company along with a copy of the latest income statement. This requirement also applies to unseparated spouses and second-degree relatives subject to their consent, whereby non-consent must be documented. When commenting this judgment, the President of the Italian SA remarked that it 'clearly points to a good practice in reconciling personal data protection and other interests as protected by the Constitution, whenever such interests happen to be in conflict with the former as part of public policies'. The President of the SA also criticised certain legislative measures, whether recent or not, which feature 'some scoffing' at the SA's call for 'respect of the proportionality principle, which must underlie any balancing between rights, freedoms and other primary goods'; he hoped that 'additional care' would be taken in future 'following the lead of the Court, in line with the reasonableness principle'. The same considerations had actually been made in the past exactly regarding transparency legislation as well as in respect of other items of draft legislation that envisaged the centralised collection of personal data – in some cases involving the whole of Italy's population and affecting the most intimate sphere of one's life. This is the case, in particular, of the 'National Data Platform' as well as of the processing operations performed by Italy's National Statistics Institute (ISTAT).

Those concerns continued in the first months of 2019, indeed additional concerns were raised in connection with implementation of blanket electronic invoicing (e-invoicing) obligations. Reference should also be made to the call recently made upon Parliament to ensure respect for the proportionality principle - for instance, in the brief submitted by the President of the SA with regard to the bill intended to enact decree-law No. 4 of 28 January 2019, which contained urgent measures on introducing the universal basic income and regulating retirement benefits. The brief was submitted on 8 February 2019 to the XI permanent committee of the Senate; an additional brief was lodged on 6 March 2019 with the joint XI and XII committees of the Chamber of Deputies, taking note of the amendments made – as requested - in the enactment process of the said decree-law. The same call for proportionality was made by the President of the SA during the public hearing held on 6 February 2019 before the joint I and XI committees of the Chamber of Deputies, in connection with the bill containing measures to ensure effectiveness of public administrative activities and to prevent absenteeism. Once again, it is the pillars of personal data protection that are impacted, which is not infrequently accounted for by the alleged need to achieve effectiveness of administrative activities. Those pillars are made up by the principles of relevance and proportionality along with the purpose limitation principle - as recalled of late by the Constitutional Court and set forth in Council of Europe's Convention 108 already prior to being enshrined in EU-related legislation. This is why one cannot but welcome the innovation brought about by Article 36(4) of the GDPR and hope that it will bear its fruits – namely, the obligation to consult the supervisory authority 'during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a

regulatory measure based on such a legislative measure, which relates to processing'. Indeed, this exercise has already been carried out successfully at domestic level several times over the past years in terms of the relationships between the SA, Parliament and the Government. The underlying rationale is to consider the Italian SA a fundamental institutional partner in order to make sure that the modernisation of Italy as based on an enhanced digital infrastructure can take place in full compliance with personal rights and fundamental freedoms.

JAPAN / JAPON

Major developments in the data protection field

1. Review of APPI

The current the Act on the Protection of Personal Information (APPI) was revised in 2015, and took effect fully on 30 May 2017. In particular, the 2015 revision of the APPI contained a provision requiring the APPI be reviewed every three years, mainly reflecting the intense progress in the information communication technologies. The APPI is currently under review, in accordance with the 2015 revision of the APPI, where the subsequent international trend on personal information protection and progress in the information communication technologies, as well as circumstances, etc., surrounding the generation and development of new industries, are taken into account.

Specifically, discussions on the necessity of the law revision are underway, in the light of the following four viewpoints:

(1) Considering the increasing concern among people about how their own information is handled and the heightening expectation in their own engagement, it is necessary to review the system, paying attention to put in place sufficient measures necessary to “protect personal rights and interests” advocated as the purpose of the Act, under Article 1 of the APPI.

(2) It is necessary that system has such a nature in which results from technological innovations brought to personal information and information related to individuals will bear fruits in both aspects of economic growth, etc., and protection of personal rights and interests, as the necessity to balance the utilization and protection, which was particularly emphasized as per the 2015 revision of the Act, continues to be important.

(3) It is necessary to review the system, paying attention to the harmony and coordination of international system, as the diverse use and application, using digitized information, have globally developed.

(4) Taking account of the progress in the use of services by overseas business operators and increasing complexity of cross-border supply chains of businesses that handle personal information, it is necessary to review and tailor the system, to fit to risks associated with such progresses, that confront individuals.

2. International activities

(1) Mutual Adequacy findings took effect between Japan and the European Union

In the light of the agreement made in July 2018 (an agreement on a policy setting out that the PPC will designate the EU and that the European Commission will make adequacy decision for Japan, respectively pursuant to the Article 24 of the APPI and Article 45 of GDPR), the framework for mutual smooth personal data transfer with the designation of the EU by Japan and the adequacy decision on Japan by the European Commission took effect as of 23 January.

The PPC expects that the effectuation of this framework will create the world's largest region where safe and smooth data flows are ensured, and that the effectuation will be an opportunity for global business corporations to generate new business models, possible enhancement of operation efficiency, cost reduction, etc., which will also result to improve consumer benefits.

Reference: Joint Statement by the Personal Information Protection Commission of Japan and the European Commission

https://www.ppc.go.jp/files/pdf/300717_pressstatement2.pdf

(2) Promotion of CBPR System

The PPC proactively works to promote CBPR, based on an understanding that APEC/CBPR System, which is a framework that certifies suitability of business operators to the APEC Privacy Framework, is an effective international standard to determine personal information protection level of business operators. The PPC held the total of 13 international seminars, etc., in FY2018, hosting approximately 1,180 participants. The PPC's domestic activities have had approximately 6,650 participants in the total of 78 presentations that the PPC organized in FY2018.

In particular, the PPC cooperated with the U.S. to hold, for the purpose of dissemination, a CBPR workshop in India in November 2018, taking into account the fact that "(they) discussed the need for the CBPR system to serve as a foundation for a globally interoperable data protection framework and committed to work cooperatively in support of interoperable privacy frameworks in international fora, and on a bilateral basis"at the ninth meeting of the U.S.-Japan Policy Cooperation Dialogue on the Internet Economy in Washington, D.C., on July 23 and 24, 2018. This workshop bore significant meaning, in the sense that it also was an opportunity for the two countries to roll out to the Indo-Pacific region, the shared efforts of promoting the CBPR system.

The PPC took part in a conference among CBPR participant economies, at the occasion of APEC's DPS meeting held this February in Santiago, Chile, where the participants discussed expanding its participation within the APEC region and possibilities to expand the CBPR participating economies to regions outside of APEC, in addition to the point that PPC considers making various efforts for the purpose of the expansions.

With the above discussions in mind, we will continuously make efforts on further facilitation of the CBPR system, in close cooperation with relevant economies, particularly the U.S.

(3) The host for international conference

The PPC hosted the 51st Asia Pacific Privacy Authorities (APPA) Forum in Tokyo from 29 to 30 May and international seminar on personal data on 3 June, entitled," The Creation of Global Free Flow of Personal data with Adequate Protection", with the hope that the event showcased discussions and information on personal information protection from countries around the world, and helped support discussions in the international forum such as G20 with the aims of enabling broad, international coordination and promoting free data flow while ensuring mutual reliability.

LATVIA / LETTONIE

After the General Data Protection Regulation (GDPR) took effect in May 2018 the Inspectorate's one of the valuable priorities was to participate in the elaboration of legal preconditions for setting up of a system for the protection of personal data of a natural person at a national level. With this aim in mind, the Personal Data Processing law entered into force 05 July 2018 in Latvia transposing the tasks in the area of protection of natural persons with regard to processing of personal data and on the free movement of such data as per GDPR.

In addition, the Inspectorate participated together with other relevant authorities in a process of drafting the implementation law in Latvia of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties, and for the free movement of such data. the process of developing and coordinating Council of Europe Framework Decision 2008/977/JHA.

During the reporting year the Inspectorate's engagement to organize a videoconferencing cycle in cooperation with the Latvian Local Government Union must be mentioned. The main goal of these events is to encourage employees of local government authorities on topical issues in the protection of personal data and, in cooperation with other public authorities, to further promote public sector awareness of the processing and protection of personal data.

So far, the Inspectorate appeared to be active in providing the information to the public about the application of the requirements of the GDPR by organizing informative seminars, public events, and participation in the "LAMP" festival on different data protection issues.

In the reference year, the Inspectorate has commenced the realization of two projects co-financed by the European Commission. The Inspectorate shall participate as one of the partners in the implementation of the European Commission Framework Programme for Research and Innovation "Horizon 2020" (Horizon 2020) for the 2016-2017 Work Programme No 786741 "For micro-enterprises TO be eligible" ("GDPR Compliance Cloud Platform for MICRO Enterprises").

The Inspectorate is also the leading partner in the "General Data Protection Regulation — Opportunities and Liability for Small and Medium Enterprises (SMEs); Rights and Risks to Minors" ("DPSME"), project 814774, the European Commission's Directorate-General for Justice, under the Financial Programme "Rights, Equality and Citizenship" for 2014-2020.

In the reference year, the Inspectorate in collaboration with other partners was involved in the sixth annual data security forum "Digital Era 2019'' on 29 May which is one of the largest events in the Baltics, devoted to the GDPR.

We hope that the information provided will be useful in your further work and we are looking forward to see you in the 38th Plenary meeting in Strasbourg.

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).

LITHUNIA/LITHUANIE

The State Data Protection Inspectorate oh the Republic of Lithuania

The State Data Protection Inspectorate (SDPI) one of personal data protection supervisory authorities in Lithuania helps to protect and safeguard the rights of citizens of Lithuania to personal data protection and privacy. In 2018 even before the official starting day of application of the new regulatory framework of personal data protection society felt a significant impact of the personal data protection reform. Society has become more self-conscious and better informed about its rights and potential risks related to their personal data processing.

In 2018 the State Data Protection Inspectorate focussed on the implementation of the priority of the personal data protection reform, namely, the development of an efficient data protection supervisory system under General Personal Data Protection Regulation. The personal data protection reform was implemented by the State Data Protection Inspectorate in parallel to its usual types of activities, which in many cases, due to General Personal Data Protection Regulation breakthrough, even exceeded the planned indicators. The new regulatory framework helps reinforcing measures aimed at securing a safer processing of personal data both in Lithuania and crossing the border.

Schengen evaluation in Lithuania. The right to personal data protection is closely related to one of the fundamental human rights of the European Union's citizens, i.e. free movement of persons within the EU. Therefore, it is necessary to ensure that Lithuania complies with its commitments assumed in relation to the Schengen area and implements requirements of the Schengen acquis for personal data protection. In 2018 the Inspectorate participated in the Schengen evaluation in Lithuania. The Schengen evaluation experts who met with the Inspectorate's representatives assessed the independence, structure, functions, funds of the Inspectorate, and the supervision of the national second generation Schengen information system and the Lithuanian national visa information system. The Schengen evaluation experts are planning to submit to Lithuania the inspection findings in the middle of 2019.

Preventive inspections. In 2018 a total of 141 preventive inspection were made. Sectoral inspections were performed in health care organisations, 12 major corporations engaged in the food, household appliances and pharmaceuticals were inspected for direct marketing and loyalty programmes purposes.

Registration of data protection officers. In 2018 there were 1,470 organisations which reported to SDPI about appointed data protection officers, out of which there were 760 public legal entities and 710 private legal entities. These could be broken down into the following main fields of activities:

- public authorities and agencies – 268;

- goods and services – 526;

- financial services – 77;

- education and culture – 281;

- health care – 182;

- law enforcement and law and order – 11;

- other – 125.

Notifications about data security breaches. In 2018 SDPI received 100 notifications about data security breaches. 93 out of this number were received after May 25th. Most of notifications were sent by companies and institutions engaged in activities related to goods and services (29 cases), public authorities and agencies (23), activities of financial services (17), activities of electronic communication services or network providers (7), health care activities (3), educational and cultural activities (1) and other activities (20). 68 investigations into data breaches resulted in 2 instructions given, 2 – recommendations, in 14 cases no violations were detected, 10 breaches were eliminated at the time of inspection, in 40 cases other measures were applied. Most of notifications were received due to the following circumstances, such as disclosure of data (56 cases), loss of data (11 cases), theft (6), data distortion (4), copying (3) and 20 other cases. With the start of application of GDPR data security breaches became relevant for all public and private sector operators. A victim of a security breach has to take actions to eliminate and record the breach, whereas in the cases prescribed in the GDPR it shall notify SDPI or people about such incidents within 72 hours from the moment it became aware thereof.

Handling of complaints. In 2018, 859 complaints were received (480 and 443 in 2017 and 2016, respectively), of which 641 complaints were lodged regarding actions by the private sector, 97 – regarding actions by public authorities, 76 – actions by other authorities, in 26 cases the party complained against had not been identified. As of May 25th, since the date of application of GDPR, many more complaints were filed. As of May 25th, 555 complaints were received. According to SDPI complaints statistics, direct marketing remains the key area of concern for the public in the field of personal data processing. Moreover, in 2018 individuals actively complained about the lawfulness of visual data processing, online data processing, data processing in the service sector and debtor's data. Various sanctions were imposed in 2018 under the LLPPD and GDPR, but no fines have yet been imposed under GDPR.

During 2018 a total of 619 complaints were handled resulting in the following sanctions:

- 141 instructions;

- 37 statements of administrative violations;

- 7 reprimands;

- 98 no violations detected.

Involvement in Policy Formation.

Drafting of legal acts. In 2018 SDPI drafted 14 legal acts (compared with 7 drafts in 2017 and 7 drafts in 2016), i.e. orders by SDPI Director mainly in the areas of operational improvements or changes in relation to GDPR application.

Approximation of draft legal acts. In 2018 while performing the function of approximation of legal acts delegated to the Inspectorate, it provided its comments and proposals within its remit on 182 draft laws submitted, on 153 draft orders, on 151 draft rules of procedure for information systems and 18 registers, on 78 draft resolutions of the Government of the Republic of Lithuania and other legal acts. The majority of draft legal acts were submitted for approximation by controllers of public institutions and bodies – 465, by controllers in health care – 58, in education and culture – 30, etc.

Performance of International Commitments.

Personal data transfer to third countries. Performance of international commitments. In 2018 SDPI issued 6 authorisations for personal data transfer to third countries. 5 requests for authorisation were rejected. In 2018 SDPI made 13 investigations to verify whether companies were following the binding corporate rules (BCR).

Opinions on draft legal documents. In 2018 SDPI analysed and drafted 54 opinions on draft legal documents deliberated by the European Commission and Council of Europe working groups and/or committees which were forwarded to the Inspectorate by the Permanent Representation of the Republic of Lithuania, ministries and other public authorities via LINESIS system. In this way the Inspectorate contributed to the EU legislative process and cases deliberated at the Court of Justice of the European Union.

International inspection. In preparation for Schengen evaluation in 2018 SDPI performed inspection of the lawfulness of personal data processing in the Embassy of the Republic of Lithuania to the Republic of Azerbaijan and Turkmenistan.

Replies to queries. In 2018 SDPI replied to 27 queries submitted by parties to the Council of Europe Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

International working groups. In 2018 SDPI representatives participated in 16 international working group meetings dealing with personal data protection. In order to become a fully-fledged member of international cooperation in the area of personal data protection the Inspectorate intensified its international cooperation activities and focused more on representation of Lithuania in personal data protection working group meetings. In 2018 the Inspectorate participated in 2 meetings of the Working Party under Article 29 of Directive 95/46/ EC and 7 meetings of the European Data Protection Board, 1 Schengen supervision coordination group meeting, 1 Eurodac supervision coordination group meeting and 1 Visa supervision coordination group meeting and in meetings of 4 other working groups.

Provision of Consultations and Information to the Public

Consultations. In 2018 SDPI provided 6,298 consultations. Out of this number, 4,234 consultations were provided to companies and institutions and the reminder 1,064 consultations – to people. In 2018 various organisations were mostly interested in the personal data protection reform. Up until 25 May 2018, 1,589 consultations were given on this subject, broken down into the lawfulness of personal data processing – 517, how to notify properly about an automated data processing – 368, lawfulness of video surveillance – 232, lawfulness of personal data provision – 217, etc. As of May 25th, majority of consultations to organisations were on issues about GDPR, LLPPD and SDPI remit – 403, on lawfulness of personal data processing – 305, on video surveillance – 173, on lawfulness of personal data provision – 160, on personal data protection officer – 159.

Public awareness. In 2018 SDPI prepared 233 public information tools. The public showed keen interest in various topics of the personal data protection reform. Information was provided to the mass media on 124 occasions, on 56 occasions SDPI participated in or gave interviews on television or radio programmes. SDPI broke 31 news on its website about relevant topics and issued 9 press releases.

Events. In 2018 SDPI representatives took part in 63 events. These were attended by 4,720 stakeholders, 77 presentations were given. Business and public sector communities were mainly informed about the personal data protection reform and latest regulatory requirements in this area.

Methodological assistance. In 2018 SDPI drafted 12 methodological documents:

In 2018 the Inspectorate prepared 9 methodological tools:

- Guidelines on appropriate organisational and technical data protection safeguards for controllers and processors;

- Recommendation to small and medium-sized businesses on application of General Data Protection Regulation;

- A standard template for data protection impact assessment;

- A recommendation on the procedure for detection, investigation, notification and filing of personal data security breaches;

- A recommendation on requirements for draft legal acts regulating personal data processing;

- A recommendation on records to be made about data processing operations;

- A reply to a FAQ regarding application of the General Data Protection Regulation for processing data about members of managing bodies of legal entities;

- A reply to a FAQ as to whether the GDPR provisions applies to natural persons who have published personal data of other individuals on the social media;

- A reply to a FAQ on how controllers should inform about an on-going video surveillance in an information table;

- Summary of results from inspections in municipal administrations regarding publishing of personal data in website sections related to on-going urban planning;

- Summary of results from inspections investigating into the lawfulness of receiving personal data from immovable property registers;

- Summary of results from inspections investigating into lawfulness of personal data processing for the purposes of direct marketing and loyalty programmes.

Survey of the Citizens of Lithuania on Personal Data Protection and Privacy Issues. The effectiveness of educational and public awareness raising activities in the area of personal data protection and privacy matters which were run by the Inspectorate in 2018 is reflected in the representative public opinion survey on personal data protection commissioned by the Inspectorate at the end of 2018 and conducted by Spinter tyrimai company. According to the survey, innovations in the regulatory framework of personal data protection and application of Regulation (EU) 2106/679 in all EU Member States as of May 25th generated enormous interest in society and organisations alike. In view of the relevance of the topic, during the survey on personal data protection the respondents were asked whether they had heard of the new personal data protection legal act which entered into force as of May 25th in Europe, including Lithuania, i.e. the General Data Protection Regulation. 71 percent of the Lithuanian citizens gave an affirmative answer to this question. People in the age group of 26–45 with higher educational background and higher income (above Eur 500) were among better informed of the new personal data protection legal act. Compared to 2016 immediately after the adoption of Regulation (EU) 2016/679, the so-called privacy paradox survey was run which yielded only 20 percent of the respondents aware of the regulation.

Also according to this survey at the end of 2018 68% of the respondents gave an affirmative answer to the question whether they were aware of or believed to be aware of their statutory rights and duties in the area of personal data protection. Compared against 35% in 2016 this demonstrates that from 2016 to 2018 a proportion of people aware of their rights and duties in the area of personal data protection

grew almost twofold. According to the 2018 survey data, larger awareness of their rights and duties in the area of personal data protection was among population from 36 to 55 years of age, hence, among people of employable age who most likely had to deal with personal data protection issues in their professional or public lives.

MAURITIUS / MAURICE

1. Guides

A. Introductory Guide on the Data Protection Act 2017

This office prepared and launched an 'Introductory Guide to the Data Protection Act 2017'. This guide has been issued to assist controllers and processors to implement the provisions of the Act. It highlights the key changes, challenges and actions that organisation should adopt in order to achieve compliance

B. Guide on Registration/Renewal

In order to address the queries effectively on the above subject, this office published a guide on its website on registration and renewal procedures. This guide has been very useful as an informative tool to the public.

C. Guide on the Roles and Responsibilities of the Data Protection Officer

The appointment of a data protection officer by controllers is mandatory according to section 22 (2)(e) of the Data Protection Act 2017. Since it is a requirement in the law, this office has received a surge of queries regarding the roles and responsibilities of a DPO and their required qualifications. To address the queries, this office has published a guide to help the organisations to better understand this topic.

D. Guide on Data Protection and Media

The Data Protection Office has prepared a guide on data protection and the media which aims at promoting the protection of the privacy rights of citizens (public figures as well as private persons) of our country. It elaborates on a general recommended approach towards compliance with the Data Protection Act (DPA) 2017 and best practices. The guide also explains how media organisations can comply with data protection principles while maintaining a free and independent role.

The guide is currently in the design and printing phase.

2. New Forms developed

As soon as the Data Protection Act was proclaimed, this office had the underpinning task of carrying to design the required forms and templates to meet the requirements of the new Act. The following forms and templates have been designed:

1. Criteria to evaluate high-risk processing operations
2. Data Protection Impact Assessments Form
3. Personal Data Breach Notification Form
4. Controller and Processor Registration/Renewal forms
5. Transfer of Personal Data Form
6. Record of processing Template
7. Template on CCTV Policy
8. Template on Data Protection Policy

3. Training Toolkit on the Data Protection Act 2017

This office is producing a corporate film on the Data Protection Office and a training toolkit to be produced on DVDs which will be distributed to controllers on the Data Protection Act. This will allow a more efficient way of training a large number of controllers/processors.

4. Benchmarking Visit from Ugandan Delegates in Mauritius

The Ugandan Parliament approached United Nations Pulse Lab Kampala to request support on best practices from the region to explore the role of data processing for sustainable development, why organisations need laws to assure legal certainty and how countries have developed compatible systems. The objective was to share lessons learned within the context of developing and least developed economies to ultimately incorporate recommendations in their national Bill. Mauritius was chosen because we have long experience of implementing data privacy and protection legislation.

To foster the exchange of ideas, UN Pulse Lab Kampala organised a visit to Mauritius for a delegation of parliamentarians and other officials from Uganda in 2018. The delegation met with key public and private sector stakeholders in the area of data protection and privacy in Mauritius. Exchanges with authorities like the Ministry of Technology, Communication and Innovation (MTCI) and the Data Protection Office as well as other relevant stakeholders from the private and government sector enabled the delegation to better understand challenges and best practices in implementing data privacy legislation from the perspective of both legislators and controllers.

5. Data Protection African Summit in Mauritius

Africa Digital Rights' Hub organised a Data Protection African Summit in Mauritius from 19 to 23 November 2018. The theme of the Summit was "Breaking New Frontiers".

The Summit brought together controllers, processors, tech companies, policymakers, regulators, innovators, business communities and individuals together to discuss and proffer solutions to the emerging issues on data protection and privacy. The main objectives of the Summit were to –

(a) influence the development of relevant national and regional frameworks for data protection;

(b) build industry capacity to ensure data protection compliance on the Continent;

(c) formulate key lessons and issues for advocacy;

(d) explore issues for regional cooperation and collaboration between African regulators, policymakers and their counterparts in the rest of the world; and

(e) showcase tools for data protection compliance.

The Data Protection Commissioner has played a supporting role in making this event happen in Mauritius to position Mauritius on the African Continent in the field of data protection.

6. African Union Workshop

This office participated in the workshop organised by the African Union on 17 and 18 December 2018. The workshop provided an overview of the main challenges and opportunities of processing personal data in Africa and its impact on the development of the Internet economy and data analytics as well as the protection of digital rights of African people. Participants from all member states were invited.

MEXICO / MEXIQUE

MEXICO'S MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD

I. CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA AND ITS ADDITIONAL PROTOCOL

1. Entry into force

On September 28, 2018, the Promulgation Decree of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereafter Convention 108), and its Additional Protocol was published in the Official Journal of the Federation. Both legal instruments entered into force on October 1st, 2018.

It should be noted that Mexico´s accession to the Convention 108 and its Additional Protocol complemented the legislative framework on this matter. This, considering that Article 133 of the Political Constitution of the United Mexican States[6] establishes that the international treaties to which Mexico is a party, along with the Constitution, shall be the supreme law of the whole Union.

The above means that the provisions of Convention 108 and its Additional Protocol are elevated to constitutional status. Therefore, when applying the current legal framework on the protection of personal data, all authorities are obliged to consider the content of both international instruments, favoring at all times the most effective protection for individuals.

The Promulgation Decrees of Convention 108 and its Additional Protocol are available at the following links: https://www.dof.gob.mx/nota_detalle.php?codigo=5539473&fecha=28/09/2018 and https://www.dof.gob.mx/nota_detalle.php?codigo=5539474&fecha=28/09/2018.

II. GUIDELINES ESTABLISHING THE PARAMETERS, MODALITIES AND PROCEDURES FOR THE PERSONAL DATA PORTABILITY

1. Legal basis

In terms of article 57 and 5th transitory of the General Law on Protection of Personal Data Held by Obligated Parties[7] (hereafter the General Law), the National Transparency System possess the necessary attributions to establish guidelines providing for the parameters to be taken into consideration to determine the hypotheses under which the presence of a commonly used structured format is presumed to be present, as well as for the technical standards, modalities and procedures for the transfer of personal data.

Therefore, on February 12th, 2018, the National Transparency System, which is presided by the National Institute for Transparency, Access to Information and Personal Data Protection (INAI), published the Agreement containing the Guidelines establishing the parameters, modalities and procedures for the personal data portability (hereafter the Guidelines). These Guidelines were approved, and they entered into force 180 days after the day following its publication in the Official Journal of the Federation.

---

[6] Available at: http://inicio.ifai.org.mx/SitePages/English_Section.aspx .

[7] Disponible en el siguiente vínculo electrónico: http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo119547.pdf, consultado por última vez el 3 de junio de 2019.

2. Objective

The purpose of the Guidelines is to establish the parameters that determine the assumptions that underlie a structured and commonly used format, as well as the technical standards, modalities and procedures for the transmission of personal data. This, in order to guarantee the exercise of the right to data portability referred to in article 57 of the General Law or those that correspond in Federal entities' legislations on this matter.

3. Thematic content

Throughout 27 articles, distributed into 4 chapters, the Guidelines contemplate the following:

- Chapter I. General Dispositions.
- Chapter II. The objective and scope of personal data portability.
- Chapter III. Specific rules for the exercise of data portability.
- Chapter IV. Technical norms and procedures for the transmission of personal data.

4. General Description

Chapter I of the Guidelines establishes its purpose and provides definitions to facilitate its technical understanding, highlighting concepts related to interoperability, metadata and personal data portability, as well as to the subjective validity, objectives and territorial scope.

The Guidelines are applicable throughout the national territory to any authority, agency, entity, body of the Executive, Legislative and Judicial Branches, autonomous constitutional bodies, administrative tribunals, trusts and public funds of the federal, state and levels, as well as political parties. This, regarding their use of systems which generate structured data formats commonly used, in order to provide data subjects with a copy of their personal data in such format for reuse and / or use, or for its transmission.

Chapter II of the Guidelines determines the criteria that must be met in order to considered that a data format is structured and commonly used, independently of the operating system used for its generation and reproduction. These criteria are:

- The format is electronic, accessible and readable by automated means, in such a manner that it can identify, recognize, extract, exploit or perform any other operation with personal data.
- The format permits the reuse or use of personal data.
- The format is interoperable with other computer systems, as long as it is technically possible.

Also, this chapter establishes the objective and scope of the right to personal data portability in accordance with article 57 of the General Law. In these terms, the data subject may request:

- A copy of the personal data which they have directly provided to the data controller, in a structured and commonly used format, which permits the continued use or delivery to another data controller for their reuse and new processing.
- The transmission of personal data to another data controller, as long as this is technically possible and the data subject has directly provided their personal data to the data controller and that their processing is based on their consent or on the signing of a contract.

Chapter II of the Guidelines punctually defines the conditions that must be updated regarding for the exercise of the right to data portability, namely:

- The processing is carried out by automated or electronic means and in a structured and commonly used format.
- The data subject´s personal data are in possession of the data controller or the data processor.
- In regard to personal data of the deceased, the interested person must proof of legal interest.
- The data subject has provided their personal data directly to the controller, actively and consciously, including personal data obtained in the context of the use, the provision of a service

or the completion of a procedure, or those provided by the data subject through a technological device.
- The exercise of this right does not affect the rights and freedoms of third parties.

Chapter II of the Guidelines expressly indicates which data could not be subject to the right to personal data portability:

- Data that is inferred, derived, created, generated or obtained from the analysis or treatment, carried out by data controller, for the personal data provided directly by the data subject, for the purpose of personalization, recommendation, categorization, profiling or other similar purposes or processes.
- The pseudonyms, unless they are clearly linked to the data subject and can identify it or make it identifiable when the data controller has additional information that allows for their individualization and identification.
- Personal data subject to a dissociation process.

Finally, Chapter II of the Guidelines establishes that the data controller is not obliged to store, preserve, keep, maintain or retain all the personal data in his or her possession in a structured and commonly used format, only for the purpose of guaranteeing the data subjects' right to data portability.

Chapter III of the Guidelines has as its objective to establish a series of specific rules that allow, from an operative perspective, the exercise of the right to data portability. Among these are the following:

- The establishment of rules related to the delivery and cost of the storage medium.
- Delivering as much metadata as possible.
- The reduction of the deadlines established to respond to a request of the data subject, as well as to make this right effective in an emergency situation.
- The rules that determine when the right to data portability becomes effective.
- The recognition of a legal remedy in the event of a refusal of the data controller to a claim of the right to data portability.

Chapter IV of the Guidelines defines the technical standards that allow the exercise of the right to personal data portability, such as:

> The implementation of mechanisms, mediums and ideal procedures that allow the data subject to obtain their personal data, done in a personal way, electronically, through download options established in data controller's official Internet page or by any other technology that it considers pertinent.
>
> Inform the data subject regarding the types of structured formats that are commonly used and that are available, through which the data subject may deliver or transmit their personal data to the data controller, depending on the nature of the personal data and the feasibility of the portability.
>
> Guarantee, as long as it is technically possible, the interoperability of a structured and commonly used format in which the personal data is delivered to the data controller or transmitted to other systems and databases.
>
> Ensure that electronic services and systems in their possession maintain the interoperability of systems, adopting protocols and standards that allow the exchange of personal data between different systems or technological platforms, regardless of the programming language or platform in which they were developed, among others.

This chapter indicates a series of technical conditions to ensure the transmission of personal data, such as: 1) To adopt protocols, tools, applications or services that allow the efficient communication of personal data. 2) To establish administrative, physical and technical security measures for the transmission of personal data in a structured and commonly used format. 3) To establish authentication mechanisms for sending and receiving personal data and to establish controls to obtain evidence about

the sending, receiving and integrity of the personal data transmitted. 4) To maintain a record of all the actions or operations related to the transmissions of the personal data.

This chapter also establishes a general procedure for the transmission of personal data. The procedure requires the following: the sending of personal data be made prior accreditation of the identity of the data subject and, where appropriate, of the identity and legal capacity of its representative; the personal data should be encrypted during its transmission to the system or electronic platform of the receiving data controller; the obligation that the transmitting and receiving data controllers authorize a person who is responsible for monitoring that the conditions, rules, procedures and applicable technical obligations, among other rules, are observed in the transmission of personal data.

The Guidelines are available at:
http://diariooficial.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018.

III. RULES OF USE OF THE LOGO OF THE INNOVATION AND BEST PRACTICES PRIZE IN THE PROTECTION OF PERSONAL DATA, PUBLISHED IN THE DOF ON JUNE 15, 2018

Objective

These rules are intended to publicize the logo of the Innovation and Best Practices Prize in the Protection of Personal Data, as well as its specifications, description, characteristics, conditions and rules for its use, to the winners of the categories provided in the call and bases of the different editions of the contest entitled “Innovation and Best Practices Prize in the Protection of Personal Data”.

The Rules are available at: http://www.dof.gob.mx/nota_detalle.php?codigo=5526625&fecha=15/06/2018

IV. PROCEDURE MANUAL FOR CARRYING OUT THE VOLUNTARY AUDITS REFERRED TO IN ARTICLE 151 OF THE GENERAL LAW ON PROTECTION OF PERSONAL DATA HELD BY OBLIGATED PARTIES

Objective

To establish the requirements and conditions, as well as the procedures, for the development of the voluntary audits as referred to in article 151 of the General Law as well as in articles 218 to 231 of the General Guidelines, that are requested to the Institute on behalf of data controllers.

The Procedure Manual for voluntary audits is available at: http://www.dof.gob.mx/2018/INAI/ANEXO-ACT-PUB-08-08-2018.06.pdf

MOLDOVA

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

In the context of the contribution on the major developments in the field of data protection in the Republic of Moldova, since the 36th plenary meeting of the Consultative Committee of the Convention for the Protection of Individuals with regard to the Automated Processing of Personal Data STE 108 (T- PD) held in June 2018, we communicate the following:

During the reference period, the Republic of Moldova continued to record constant and progressive steps on the personal data protection dimension. This period is characterized both by the tendency to harmonize the legislative framework of the Republic of Moldova with the aquis communautaire on the protection of personal data, to raise the awareness of the personal data subjects as well as to inform the personal data controllers, establishing inter-institutional partnerships with authorities of the Republic of Moldova in order to develop a fruitful cooperation on the personal data protection dimension, etc.

1. Development of legislative acts

The major evolution registered in the field of personal data protection represents the adoption by the Parliament of the Republic of Moldova in the first reading of the draft Law on personal data protection.

The draft law aims at strengthening the legislative system to ensure respect for constitutional law, the inviolability of private life by bringing the system of national law into line with the Community law in the field of reference, namely the provisions of Regulation (EU) 2016 / 679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) and Directive EU 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of the prevention, detection, investigation or prosecution of criminal offenses or the execution of penalties and on the free movement of such data and repealing Council Framework Decision 2008/977 / JHA.

This development draws a continuous line of compatibility between the rules of the internal law and the provisions of the Community law in the field of personal data protection. It will contribute to the fulfillment of the commitments assumed by the Republic of Moldova in relation to the European Union and the recognition of the appropriate level of personal data protection in the Republic of Moldova under domestic law and international commitments. It will also make possible the transfer of personal data to the Member States of the European Union or to other states recognized as providing an adequate level of personal data protection, without any other additional security measures from the Republic of Moldova.

In the same context, the scale of major developments in the field of personal data protection is further determined by the adoption by the Moldovan legislator in the first reading of the draft Law on the National

Center for Personal Data Protection, which aims at consolidating and strengthening the functional competencies of the national supervisory authority of personal data processing.

2. Data protection activities organized within the Twinning project "Strengthening the Capacity of the National Center for Personal Data Protection"

During the reporting period, the Center continued to implement the Twinning project, which is funded by the European Union and implemented by the German Foundation for International Legal Cooperation (IRZ) and the Ministry of Justice of the Republic of Latvia. The project is an important contribution to the EU-Moldova Association Agreement**.**

The activities held aimed at harmonizing the national legislation of the Republic of Moldova in the field of personal data protection with that of the European Union, in particular the General Data Protection Regulation (UE / 2016/679) and Directive 2016/680. Thus, the planned actions were carried out with the support of 20 EU experts focusing on:

- Individualized recommendations on the new draft law on personal data protection and the draft law on the National Center for Personal Data Protection.
- Elaboration of GDPR Impact Study on Private Companies in the Republic of Moldova;
- Organizing training sessions for personal data controllers and private companies on the implementation and impact of GDPR. At the end of the training, each participant received a certificate signed by the Center and the Twinning project. In total 190 representatives of private companies attended the trainings.
- Organizing training sessions for state institutions, mass media and NGOs on data protection in different areas of activity.
- Providing methodological support for the development of operational documents of the Center (internal instructions).
- Development and delivery of a training for Center's staff focused on communication and awareness building on personal data protection.
- Assistance in the development and implementation of manuals (standard operating procedures) for Center's staff on:

a) Impact assessment
b) Monitoring and prevention
c) Investigations
d) Complaints
e) Trans-border transfer.

- Assistance in the development and/or harmonization of sectoral law and secondary legislation with the view of rendering them compliant with the new draft law on personal data protection.
- Assistance in development of 7 codes of conduct and / or guidelines for processing personal data in specific sectors (health, finance, law enforcement, electoral process, media, video surveillance and electronic communications).

3. Participation in international data protection forums

During the reference period, the Center management and staff participated in a number of international events (meetings, working groups, conferences) provided within the activities organized both by the Council of Europe and the Data Protection Authorities.

In order to be updated with the best practices and to exchange experience in the field of data protection, we communicate that the Center regularly participates in plenary sessions of the European Data Protection Board (EDPB) and other international meetings in the field of data protection. In this context, we mention participation in:

- Plenary meetings of the European Data Protection Board.
- Subgroups of the "European Technology Committee", "Social Media", "Enforcement", which took place in Brussels.
- The 40-th International Conference on Data Protection and Commissioners' Confidentiality held in Bulgaria.
- The Regional Conference on Cybercrime Strategies and the final meeting of the Cybercrime @ EaP project, held in Tbilisi, Georgia.
- Third MSI-AUT meeting, held in Strasbourg, France.
- The Spring Conference of the European Data Protection Authorities in Tbilisi, Georgia.

The gradual change in the legislation of the Republic of Moldova in the field of personal data protection is a major step towards the recognition of the Republic of Moldova as a state providing an equivalent level of personal data protection with the one of the European Union.

MONACO

Développements majeurs intervenus sur les 12 derniers mois en matière de protection des données personnelles juin 2018/juin 2019

°°°

- Signature, le 10 octobre 2018, du protocole d'amendement modifiant la convention 108 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

LOI

- - Loi n° 1462 renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption

PROJETS DE LOI

- Projet de loi n° 992 relative à l'identité numérique

- Projet de loi n° 994 modifiant la loi n° 1.383 du 2 août 2011 sur l'économie numérique

RECOMMANDATIONS DE L'AUTORITE DE CONTROLE - CCIN

- Recommandation du 16 mai 2019 sur la sécurité devant entourer les cartes de paiement en matière de vente de biens ou de fourniture de services à distance ainsi que les sites web ;

- Recommandation du 16 mai 2019 sur les modalités de dépôt et la durée de conservation des cookies et autres traceurs sur les terminaux d'utilisateurs de réseaux de communication électronique.

NORWAY / NORVEGE

The new Personal Data Act of 15 June 2018 no. 38 on the processing of personal data entered into force on 20th July 2018. The Act implements Regulation (EU) 2016/679 (General Data Protection Regulation) into Norwegian law and provides further supplementary provisions on the processing of personal data. In addition to the general rules in the Personal Data Act, various sector-specific rules on the processing of personal data have been adopted, including with regard to health services, the working environment and immigration.

POLAND / POLOGNE

Country report on major developments in the data protection field The Personal Data Protection Office (UODO)

2018/2019

I. Legislation

1. Recent National Developments – legal framework

On 6 February 2019, the Act of 14th December 2018 on the protection of personal data processed in connection with the prevention and combating of crime (Journal of Laws of 2019 item 125) implementing the Directive 2016/680, came into force. The Act concerns the definition of acceptable goals, the definition of personal data processing, regulations regarding the personal data processing and the rights of data subjects, defining tasks and requirements for the controller, processor and data protection officer. The subject of the Act is to regulate the issues related to the processing of personal data by competent authorities in connection with activities related to the prevention and combating of crime.

Moreover, in order to harmonize the provisions of 168 Polish acts with the GDPR, the Act of 21st February 2019 on the amendment of certain acts in connection with ensuring the application of the Regulation (EU) 2016/679 of the European Parliament and of the Council was passed by the Polish Parliament. These changes are aimed at removing regulations that are in contrary or duplicate solutions contained in the GDPR. The purpose of the amendment is, however, to adapt the solutions provided in the GDPR to the specificity of the Polish legal order. The Act introduces numerous changes in sectoral laws, including: Insurance, Banking, Culture, Health, Family and Labour, Internal Affairs and Administration, Environment, National Education, Investment and Development, Entrepreneurship and Technology, National Defence, Justice, Infrastructure.

Additionally, the Announcement of the President of the Personal Data Protection Office of 17th August 2018 regarding the list of the kind of processing operations which are subject to the requirement for a data protection impact assessment was published in 'Monitor Polski' – the Official Gazette of the Government of the Republic of Poland. The list contains 9 categories of processing operations for which it will be mandatory to make data protection impact assessment, examples of operations presenting high risk to the rights and freedoms of natural persons and examples of potential areas covering these operations.

2. New President of the Personal Data Protection Office

On 4 April 2019 the Sejm – the lower chamber in the Polish Parliament – appointed Jan Nowak as the new President of the UODO. His four-year term of office began from the day of taking the oath before the Sejm, i.e. on 16 May 2019, in accordance with the Act on the Personal Data Protection.

II. Events

On 3-4 July 2018 Personal Data Protection Office along with the Cardinal Wyszyński University in Warsaw, the University of Warsaw and International Centre on Law, Life, Faith and Family co-organised International Conference on Human Rights: Evaluation and Future Directions'. The event was held on the occasion of 70th Anniversary of the Universal Declaration of Human Rights and the 25th Anniversary of the Ratification of the European Convention of Human Rights by the Republic of Poland under the Honorary Patronage of the Minister of Foreign Affairs of the Republic of Poland.

On 30 July 2018 the Polish SA along with European Law Students' Association ELSA Poznań co-organised the International Conference on „Legal aspects of personal data protection in cyberspace" within the framework 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".

On 21 September 2018 the Office organized seminar ’Data protection by design – the GDPR requirements in software development’. The event was addressed to people involved in software development processes. The seminar concerned the current legal situation regarding the personal data protection with particular emphasis on its impact on IT systems.

On 28 September 2018 the UODO was a co-organiser of the 3rd National Conference ‘"Challenges and directions in registration of civil status after three years of validity of new regulations" along with the Catholic University of Lublin and the Ministry of Internal Affairs and Administration.

In 2019, just like in previous years, the UODO celebrated, already for the 13th time, the European Data Protection Day. As each year, activities were devoted to most recent issues related to the right to privacy and data protection. All of them were organized by the UODO or other institutions in cooperation with the UODO and with active participation of the UODO’s representatives, including inter alia:

- 28 January 2019, Warsaw – Conference "Personal data protection system after the introduction of the reform" - the main point of celebration of the 13th Data Protection Day. The topics discussed during the event were: telemarketing and implementation of the rights of people on the Internet.
- January – February 2019 – A nationwide social campaign on network security organized by Śląska Sieć Metropolitalna in partnership with the City of Gliwice under the patronage of the UODO.
- 1 February 2019, Dąbrowa Górnicza – the 5th edition of the Open Day of Personal Data Protection Office at the Academy WSB in Dąbrowa Górnicza.

III. Educational activities

1. Educational activities

The Polish DPA continued its diversified educational activities addressing different groups. The main focus was on data protection officers. In the reporting period, the Polish SA held several seminars on:

- ‘Employers' obligations in the field of personal data protection’ (4 October 2018)
- ‘Personal Data Protection Impact Assessment for data protection officers’ (19 December 2018)
- ‘Notification of a personal data breaches’ (14 January 2019)
- ‘Transfers of personal data to the third country’ (11 February 2019)
- ‘The rules of data processing in the light of the act implementing Directive 2016/680, addressed to data protection officers’ (12 February 2019)
- ‘Information obligation’ (28 February 2019)

On 27-29 June 2018 the Office inaugurated educational campaign for local government units on Application of the new law on the personal data protection. The events were addressed to the employees responsible for the personal data protection in local government units. During each meeting expert from the Polish SA discussed the most important elements of the GDPR.

On 19 September 2018 the Office organized a Workshop on codes of conduct for representatives of communities working on the creation of codes.

From September 2018, in cooperation with the National Institute of Freedom, the Polish SA’s continued trainings for NGO’s called ‘Ready for the GDPR’. The aim of trainings was to explain how the entities in this sector are to protect personal data. The educational campaign included a series of free trainings. They started in April, ended in October 2018 and covered all capitals of the Voivodeships. The aim of these trainings was to familiarize representatives of NGOs from all over Poland with the obligations imposed on them in accordance with the GDPR.

On 30 November 2018 the Personal Data Protection Office organized a seminar ‘Artificial intelligence is a thief of your personal data’. The event was an opportunity to discuss the benefits, but also the risks associated with the processing of personal data by computer systems simulating human thinking.

The Polish SA was also responsible for the 9th edition of the essay on data protection competition. The theme of this year's competition was ‘Sharing personal data of students to their family members’. The purpose of this competition is to promote data protection among law and administration students, and raise awareness about the GDPR.

On 26 March 2019 the Office held an academic seminar with students from several Polish universities on the protection of our data and privacy. During the meeting the President of the Office discussed with students the ways of respecting the right to privacy and the personal data protection.

The President of the Personal Data Protection Office met also with children from the primary classes a month earlier on 20 February 2019. The topics of the meeting included the privacy, anonymity and data protection rules.

In the reporting period, the Polish SA published guides to explain the GDRP regulations in a friendly way, addressing them to individual groups:

- ‘Protection of personal data at the workplace. Guide for employers’- the guide indicates how to process the personal data both during recruitment and the whole period of employment.
- ‘Protection of personal data in the election campaign’ - the guide indicates what are the basic principles of personal data processing. It emphasizes the importance of the role of the controller, which is the entity deciding on the purposes and methods of data processing, and indicates that various controllers process data at various stages of the election campaign.
- ‘Ready for the GDPR’ - for the needs of the "Ready for the GDPR" campaign, a free textbook for NGO’s was developed.
- ‘Personal data protection in schools and educational institutions’ - The Personal Data Protection Office in cooperation with the Ministry of National Education prepared a practical guide regarding the personal data processing in schools and educational institutions. It contains updated tips on the processing of personal data of children, their parents and legal guardians, teachers, as well as other employees of schools and educational institutions.

2. Projects and programmes

Within its educational activity, the Polish DPA is inter alia involved in national and international projects:

- T4DATA - a transnational project that aims to provide support for training of data protection supervisory authorities and the data protection officers of public bodies on the practical implications and possible interpretations of the GDPR. The second transnational training was organized by the Personal Data Protection Office in cooperation with the project coordinator - the Italian foundation Fondazione Basso for the representatives of public administration. The meeting took place in Warsaw on 8-10 October 2018.

  On 27 and 31 May 2019 the Personal Data Protection Office in cooperation with National Institute for Local Self-government organized local trainings entitled: "Changes in the protection of personal data in the light of the GDPR and the Act of 10 May 2018 on the Protection of Personal Data". The initiative was addressed to data protection officers as well as to the leading figures who perform this function in public administration.

- ’Erasmus + "e-OpenSpace: EUROPEAN INNOVATIVE OPEN PLATFORM’ - the Polish SA 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 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. As part of this project, a conference summarizing the year of application of the GDPR was held in Warsaw on 30 May 2019.

- „Your Data – Your Concern" - The Poland-wide Educational Programme the main objective of which 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 9th edition of the programme is conducted.

IV. Decisions and others

- *On 6 April 2019 the President of the Personal Data Protection Office imposed – by way of a decision - the first fine in the amount of over EUR 220 000 for the failure to fulfil the information obligation. The fined company did not meet the information obligation in relation to over 6 million people. Out of about 90 000 people who were informed about the processing by the company, more than 12 000 objected to the processing of their data. (ZSPR.421.3.2018)*
- On 25 April 2019 the President of the Personal Data Protection Office imposed – by way of a decision - the second fine in the amount of over EUR 13 000 for the failure to ensure the security and confidentiality of processed personal data of people who have been granted a judge's license in 2015; the failure consisted in unauthorized disclosure of personal identification number and address of their residence on the website. (ZSPR.440.43.2019)
- Sectoral Inspection Plan for 2019: According to the annual plan of sectoral inspections approved by the President of the UODO, the Office verifies personal data processing in areas such as: telemarketing, profiling in banking and insurance sector, the waste identification and video surveillance. This year the UODO takes a closer look at entities such as: Police, Border Guard and detention centres, checking their use of technical and organizational measures aimed at preventing unauthorized access, copying, changing or deleting data.
- The Office has launched a special helpline dedicated to data protection officers.

V Agreements on cooperation

On 10 May 2019 the President of the Personal Data Protection Office in Poland and the DPO of the Catholic Church concluded a cooperation agreement. The agreement delineates the principles, scope and form of cooperation between the President of the UODO in Poland and the Data Protection Officer of the Catholic Church - an independent supervisory authority in the field of personal data protection of the Catholic Church, which concerns the implementation of the tasks provided for by law of both bodies in line with their independence and competences.

PORTUGAL

No new legislation concerning specifically the protection of personal data was published during the period going from 19 June 2018 to 5 of June 2019. However two new laws were enacted that, within the framework of their specific subjects, do have relevant dispositions concerning the protection of personal data.

One of the laws makes some changes to the Penal Code criminalising some divulgation of personal data against the will of the concerned person through Internet; the other concerns specifically the role of consent in what the care of people facing terminal illness are concerned.

Law No. 31/2018, of 18 July

Rights of persons in the context of advanced disease and end-of-life

Article 5

Informed consent

1 - Persons in the context of advanced disease and end-of-life are entitled to consent, contemporaneous or anticipated, to the clinical interventions they are subject to, provided they have been previously informed and clarified by the attending physician and by the accompanying multidisciplinary team.

2 - The consent foreseen in the preceding paragraph shall be provided in writing in the case of interventions of a more invasive nature or involving a greater risk to the patients' well-being, and must be provided in writing and before two witnesses when there is the possibility of an intervention that could jeopardize their lives.

3 - Persons in the context of advanced disease and end-of-life, provided that they are adequately informed of the foreseeable consequences of this option by the attending physician and the accompanying multidisciplinary team, are entitled to refuse, under the law, artificial support of vital functions and to refuse to receive treatments that are not proportionate or adequate to their clinical condition and treatments of any nature, which do not aim solely at reducing suffering and maintaining the patient’s comfort or which prolong or aggravate such suffering.

Law No. 44/2018, of 9 August

Reinforcing the legal protection of privacy on the Internet (the forty-sixth amendment to the Criminal Code, approved by Decree-Law no. 400/82 of 23 September)

«Article 152

[...]

1 — . . . . . .

2 — In the case provided for in the preceding paragraph, if the agent:

a) Practices the act against a minor, in the presence of a minor, in the common domicile or in the domicile of the victim; or

b) Disseminates, through the Internet or other means of widespread public dissemination, personal data, such as image or sound, relating to the privacy of one of the victims without their consent; shall be punished with imprisonment from two to five years.

3 — . . . . . .

4 — . . . . . .

5 — . . . . . .

6 — . . . . . .

Article 197

[...]

The penalties provided for in Articles 190 to 195 shall be increased by one third in their minimum and maximum limits if the fact is practiced:

a) . . . . . ; or

b) Through the media, or through the Internet, or through other means of widespread public dissemination.»

SERBIA/ SERBIE

Serbian contribution on the major developments in personal data protection since June 2018

Legislation

1. Recent National Developments –legal framework

Serbia adopted new Law on Personal Data Protection (Official Gazette RS 87/2018) which entered into force on 21 November 2018 and will take effect upon expiry of nine months from the date of entry into force of the Act, except the provisions of Article 98 of this Act (which refers to the Central Registry data collections) which is applied from the day entry into force of the Law. The Law combines provisions of GDPR and the Directive (EU) 2016/680. Prescribed penalties are in accordance with domestic laws. In order to fully implement the Law, Government and the Commissioner should adopt numerous bylaws by 21st August 2019. Commissioner has the obligation to adopt 13 bylaws and further 3 bylaws may be adopted (but there is no such obligation). The Government has to adopt one bylaw.

Commissioner for Information of Public Importance and Personal Data Protection Rodoljub Sabic ended his mandate in December 2018. Until June 2019, the new Commissioner has not been elected in the Parliament.

SLOVENIA / SLOVENIE

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD (2018)

Report by the Information Commissioner of the Republic of Slovenia

A. Summary of activities

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

In 2018, the IC focused on the effective enforcement of the new General Data Protection Regulation (hereinafter "GDPR") in terms of raising awareness, making comments in the process of drafting a new act on data protection and reorganizing as well as strengthening the authority.

In 2018, the IC initiated 1029 inspection cases, 330 in the public and 699 in the private sector, which represents a 57% increase compared to previous year. A significant increase in the number of complaints is undoubtedly the result of greater awareness of individuals, since there was a lot of media attention focused on the GDPR. However, the IC issued only 20 fines and 22 admonitions in these procedures because of the absence of procedural rules for imposing administrative fines under the GDPR in the Slovenian legal order. Both, complaints and offences mainly concerned unlawful processing of personal data, inadequate data security and inadequate traceability of data processing, unlawful collection and further processing of data, noncompliance with contractual processing provisions, unlawful video surveillance and direct marketing.

In addition to the inspection and offence authority competences the IC performs other tasks. 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 2018, the IC issued 2192 written opinions and clarifications and gave more than 3230 clarifications over the phone. The IC is also competent to conduct prior checks regarding biometric measures (4 new cases in 2018), transfer of data to third countries (12 cases in 2018) and connection of filing systems (14 cases in 2018). Additionally the IC issued more than 60 opinions on legislative proposals.

The IC is also the appellate authority regarding access to an individual's personal data. In 2018, the IC received 106 complaints from individuals regarding infringements of the right of access.

Last but not least the IC participated in a number of cross-border cooperation cases in 2018, namely in 81 procedures for determining lead and concerned supervisory authorities, in 30 "one-stop-shop" procedures and in 6 procedures for mutual assistance. Cases in cross-border cooperation mainly concern multinational online businesses, i.e. Facebook, Google, Twitter, LinkedIn, Amazon, Apple, etc. and the compliance of their practices with the GDPR in various areas.

B. Information on interesting case-law

1. Photographing children at events in schools and kindergartens

The IC received numerous questions from concerned parents, elementary schools and kindergartens regarding the permissibility of photographing children's performances at school events by parents in relation to GDPR. In a press release, the IC stressed that there were no major changes to the aforementioned after the enforcement of the GDPR. As a general rule, the photographing or recording of children by parents constitutes a processing of personal data carried out for personal or private use, and therefore, according to Article 2(2)(c) of the GDPR, does not constitute a breach of the PDPA and the GDPR. The IC considers that the measure of some educational institutions that absolutely prohibited parents from photographing or recording their children at a school or kindergarten event (allegedly on the basis of GDPR) was not

appropriate. Parents, however, must be careful not to provide photographs of other children to third parties without the consent of their parents.

If a school or kindergarten event is recorded or photographed by a school or kindergarten itself, the latter is considered to be the controller and therefore has to obtain consent form children's parents or other legal representative for such processing. However, if there is a public event, the organizer of the event (school, kindergarten) does not have to acquire personal consents of the participants for general photographing of the event, provided that it informs the participants in advance of the recording and publishing of the recordings in an appropriate manner (information referred to in Article 13 of the GDPR). Any individual who participates in a public event must be aware that at such an event there is a greater likelihood that it will be recorded and that the photo will be published in different media in order to present the event itself.

2. Video surveillance in work areas and monitoring live camera images

In the inspection procedures, the regulation of access rights to the video surveillance system and the access to the live image proved to be problematic. In most cases, the employers have access to the live image and they monitor the live picture at their discretion and contrary to the purpose of video surveillance, mainly in order to supervise the work of individual workers. However, such conduct does not comply with Article 5(1)(b) of the GDPR, which stipulates that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The IC believes that employers who perform video surveillance within work places must designate persons who have access to the video archive and, in exceptional cases, also a person who will monitor a live image in accordance with the legitimate purposes of the video surveillance. Authorized persons may also look through the video archive, but only in accordance with the purposes set by the PDPA for the video surveillance, while ensuring the proper traceability of video insights. Looking through a video archive or monitoring a live image solely for the purpose of controlling employees constitutes a personal data breach and interferes with the right to privacy of employees to which they are entitled at the workplace.

3. Illegal access to medical personal information

The IC receives several applications annually regarding the suspicion of illegal access to medical personal information in which individuals also wish to obtain a list of persons who processed their personal data. In the case of a confirmed suspicion of unlawful access to information about the health condition which, according to Article 9(1) of the GDPR, is considered to be a special category of personal data, the IC shall normally impose a fine on the offender. Employees in a medical institution can only access the patient's personal data if they participate in the process of medical treatment or for other legitimate reasons (e.g. for the purpose of issuing an invoice for the performed medical services or for the purpose of mandatory reporting certain cases to the police). Some individuals whose personal names are recorded in the traceability logs of personal data processing and did not have a legitimate reason for access to personal data, would like to avoid liability by claiming that they did not access the data but someone else using their password did. In such a case the IC also fines data controllers, however not because of the illegal processing of personal data, but due to inadequate password protection.

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). Together with the Centre for Safer Internet of Slovenia it covered awareness rising activities for children and youngsters. The IC was also present on the LinkedIn and the Facebook, trying to raise the awareness of the importance of personal data protection through his profile.

In 2018, the IC strengthened the field of work in the area of compliance, prevention and information technologies. In this field, experts with legal, technological and communicational know-how are required to properly prepare materials and communicate with persons concerned.

The experts of the IC also (altogether) conducted 109 pro bono lectures in 2018. In addition, the IC published new guidelines on various data protection topics: transfers of personal data to third countries or international organisations, processing by a processor, data protection impact assessment, privacy policy and protection of personal data of consumers.

In terms of policy issues the IC has dealt extensively with, the GDPR and the accompanying Law enforcement Directive 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 and now European Data Protection Board in this regard, as well as contributing to the national discussions regarding implementation of the new EU data protection framework.

In the context of the European Data Protection Day 2018 the IC hosted a round table dedicated to the practical experiences in implementation of the GDPR. At the event, as per tradition, the annual awards for Privacy Ambassador and ISO/IEC 27001 (information security standard) were presented to selected data controllers.

The IC also participated in a number of international events and bodies such as: European Data Protection Board and its expert subgroups, Schengen Information System II Supervision Coordination Group, Europol Cooperation Board, Visa Information System Supervision Coordination Group and Customs Supervision Coordination Group, EURODAC Supervision Coordination Group, International Working Group on Data Protection in Telecommunications (IWGDPT), Council of Europe's Consultative Committee under the Convention 108 (T-PD).

At the end of 2018 the IC started implementation of a European project RAPiD.Si (Raising Awareness on Data Protection and the GDPR in Slovenia), the main purpose of which is education and awareness of small and medium-sized enterprises and individuals on the reform of the legislative framework for the protection of personal data. The RAPiD.Si project is co-financed by the European Union and will last until September 2020. Within the project, a new website "www.upravljavec.si" was made, offering answers to the most common questions, asked by craftsmen and small businesses. One of the project activities for small businesses is also free telephone hotline for SMEs.

Furthermore, the IC attended the second meeting of the »Initiative 20i7« in Macedonia in April of 2017. At this meeting, the chairs of the supervisory authorities for the protection of personal data from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Kosovo, Macedonia and Slovenia discussed the challenges that arise at the national level regarding the implementation of the new European standards for the protection of personal data.

The experience of the first year of application of the GDPR shows that the direct application of its provisions presents a major challenge, which will require considerable attention also in the coming years. In particular, given that Slovenia has not yet transposed the Law Enforcement Directive to its legislation and has not adopted rules for the implementation of the GDPR. In practice this means a number of legal uncertainties for companies and other organizations, for the exercise of individual rights as well as for exercising supervision and imposing administrative fines under the GDPR.

SWITZERLAND / SUISSE

Développements majeurs survenus dans le domaine de la protection des données

Information sur les développements majeurs survenus dans le domaine de la protection des données en Suisse

En cette première partie d'année 2019, trois points particuliers peuvent être mis en avant en ce qui concerne les développements majeurs survenus dans le domaine de la protection des données en Suisse: En effet, durant cette année les autorités de protection des données de la Confédération et des cantons ont abordé les défis communs qui les attendent en matière d'élections, de police et de numéro AVS (numéro social d'assurance vieillesse et survivants). Elles ont publié un guide consacré à l'élection du Conseil national; par ailleurs, la nouvelle loi sur la protection des données Schengen est entrée en vigueur le 1er mars 2019. Enfin une modification législative doit en outre permettre à toutes les autorités d'utiliser systématiquement le numéro AVS.

Protection des données plus stricte dans le contexte politique

2019 est une année électorale. Les élections organisées par les cantons pour le renouvellement du Parlement fédéral et des parlements cantonaux se déroulent dans un environnement numérique caractérisé par des procédés de traitement de données qui sont en constante mutation et qui ne restent pas sans effets sur le comportement des électeurs. Avec leur guide du 1er décembre 2018 concernant le traitement numérique de données personnelles dans le cadre d'élections et de votations en Suisse, les autorités de protection des données de la Confédération et des cantons ont apporté leur contribution à la libre formation de l'opinion des citoyens et des citoyennes et à l'expression fidèle et sûre de leur volonté, garanties par la Constitution. Le guide en question enjoint aux partis politiques, ainsi qu'aux prestataires de services et aux réseaux sociaux qui œuvrent en leur faveur, de rendre claires et compréhensibles les interventions numériques destinées à influencer la volonté des électeurs. Le traitement de données à des fins politiques est soumis à un niveau de protection plus élevé que celui qui s'applique aux activités commerciales. Les citoyens suisses ne doivent pas être induits en erreur par des indications fausses ou trompeuses concernant les expéditeurs et les sources des messages politiques. Ils ont le droit de savoir s'ils communiquent avec un être humain ou avec une machine (« *social bots* »). Ils ne doivent pas non plus être laissés dans le vague quant au recours éventuel à l'intelligence artificielle, ni quant à l'enrichissement ou à l'exploitation, à des fins politiques, d'informations tirées des médias sociaux (« *social match* »). (cf. Guide relatif aux élections : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/Wahlen.html)

Surveillance renforcée des activités policières

La nouvelle loi sur la protection des données Schengen est entrée en vigueur le 1er mars 2019. Cette nouvelle loi fédérale – et l'adaptation correspondantes des législations cantonales relatives à la protection des données – constituent pour la Suisse, en tant que membre associé à Schengen, la mise en application des adaptations apportées à ce qui se nomme l'« acquis de Schengen ». Elles obligent les autorités de poursuite pénale de la Confédération et des cantons à recourir à de nouveaux instruments de travail, comme l'analyse d'impact relative à la protection des données personnelles et l'annonce des violations de la protection des données. Elles confèrent par ailleurs aux autorités de protection des données de la Confédération et des cantons des compétences de surveillance accrues, par exemple celle de prononcer des décisions. Ces prochains mois, la surveillance exercée par ces autorités sur les organes de police de la Confédération et des cantons revêtira entre autres une fonction pilote : les nouveaux instruments inscrits dans la loi sur la protection des données Schengen sont destinés à être

étendus par la suite, dans le cadre de la nouvelle loi fédérale sur la protection des données (LPD), actuellement débattue au Parlement fédéral, aux traitements de données effectués par des particuliers, ainsi qu'aux traitements effectués à d'autres fins.

Utilisation systématique du numéro AVS comprend des risques pour la protection des données

Dans une adaptation de la loi fédérale sur l'assurance-vieillesse et survivants, le Conseil fédéral a prévu d'autoriser les administrations fédérales, cantonales et communales à utiliser systématiquement le numéro AVS (numéro social d'assurance vieillesse et survivants) comme identifiant unique en dehors du domaine des assurances sociales. De l'avis des autorités de protection des données de la Confédération et des cantons, le projet du Conseil fédéral présente de sérieux risques pour la protection des données, auxquels celui-ci entend y opposer des prescriptions concrètes relatives à la protection des données, comme l'obligation de procéder périodiquement à une analyse d'impact des risques. Les autorités de protection des données de la Confédération et des cantons voient ces prescriptions d'un œil favorable ; elles auraient toutefois préféré que le Conseil fédéral ait fait reposer son projet sur un concept de sécurité pour les identifiants des personnes (postulat 17.3968 du Conseil national).

SLOVAKIA / SLOVAQUIE

The Office for Personal Data Protection of the Slovak Republic has organised The Data Protection Day 2019 in form of conference open for public. The conference tackled important topics, such as data protection in school environment, duties of processors when using CCTV systems etc. We are also included in ongoing debates on Protection of Children in Online Environment, Online Strategic Plans for Slovakia and e-health debate, in which we are in the position of data protection watchdog. Also, we participate in other debates with public bodies and cooperate with them in order to achieve data protection environment in Slovak Republic compatible with high legislative standards. Our employees attend various conferences and seminars, where they give presentations on data protection topics. In the near future, we plan to organise seminars on Data Protection at Schools and Kindergardens. Beside above mentioned activities, we support our employees in self- eductaion, we oraganise internal seminars in our Office with data protection topics as well as soft skills mostly used in their professional life. Currently, work on project, which should improve our Office (better services such as webpage, more financial and persnal resources...).

TUNISIA/ TUNISIE

DEVELOPPEMENTS MAJEURS DANS LE DOMAINE DE LA PROTECTION DES DONNÉES

La protection des données personnelles en Tunisie continue à se renforcer dans un pays en transition démocratique. On se contentera de citer les développements majeurs depuis la dernière réunion du comité en 2018 et qui tournent autour de sept axes principaux.

I. Cadre juridique de protection, en amélioration constante

La Tunisie, pays précurseur dans sa région africaine et arabe avec la constitutionnalisation de la protection en 2002, l'édiction de la première loi depuis 2004 et la mise en place en 2008 de la doyenne des autorités de protection dans sa région, se devait d'améliorer le cadre juridique de protection des données personnelles.

La **ratification de la convention 108** du Conseil de l'Europe en mai 2017 a permis conformément à l'article 20 de la constitution tunisienne de lui donner une force supérieure à la loi nationale. Ainsi plusieurs dispositions de la loi furent modifiées ou abrogées par le simple fait de l'entrée en vigueur de ladite convention : Les articles 53 et 54 qui faisaient bénéficier les structures publiques d'un régime dérogatoire ou l'article 16 qui en faisait de même pour les employeurs.

Le deuxième acquis, a été l'édiction à l'initiative de l'INPDP de la **circulaire du Chef du Gouvernement** (numéro 8 en date du 22 février 2019) relative à l'utilisation par les structures publiques des données de la carte d'identité nationale. Ces données personnelles étaient collectées et diffusées publiquement, ce qui portait atteinte à la protection de données et ouvrait la voie à des cas courants d'usurpation d'identité.

Le troisième acquis s'inscrit au niveau de l'élaboration des **textes législatifs et règlementaires**. Ceux-ci incluent maintenant dans leurs visas et dans leurs dispositions la référence à loi nationale et la ratification de la convention 108 à l'image du décret gouvernemental du 6 mai 2019, relatif à l'application de l'article 30 du code des collectivités locales ou la circulaire numéro 8 *précitée.*

La quatrième réalisation, concerne le **nouveau projet de loi organique** sur la protection des données personnelles. L'INPDP, consciente du caractère universel de la protection des données et de la nécessité de rehausser le niveau de protection en Tunisie, a été à l'origine du projet intégrant les principes du RGPD. Approuvée par le gouvernement en mars 2018 il bénéficia de la priorité d'examen au Parlement. L'INPDP a réussi à faire programmer l'étude finale de ce projet au sein de la commission parlementaire à partir du 11 juin 2019.

Enfin la dernière action a été la mise en œuvre par L'INPDP de son pouvoir réglementaire à travers l'édiction de **trois délibérations** : la première, à la veille des élections municipales de 2018, relative à la protection des données dans le cadre de l'activité politique, la deuxième et la troisième en septembre 2018, concernant d'un côté la protection des données dans le domaine de la santé (qui reprend les dispositions principales de la recommandation du Conseil de l'Europe) et d'un autre côté la vidéo protection.

II. Implication de l'autorité judiciaire pour une meilleure protection

L'Instance ne bénéficie pas du pouvoir de prendre des sanctions contre les responsables de traitement non respectueux de la loi, elle se limite à saisir la justice judiciaire. Les tribunaux étant submergés par la masse de dossiers et les magistrats très peu formés aux questions de protection des données personnelles, ont fait que quatre-vingt-dix pour cent des affaires transmises par l'instance depuis sa création, jusqu'à fin 2018, n'ont pas été jusqu'à ce jour jugées.

La fin de l'année 2018 a été marquée par un léger changement sur ce plan. En effet, la justice a condamné en septembre 2018 un responsable de traitement qui a installé un système de vidéo protection sans autorisation préalable de l'INPDP. D'un autre côté, la cour d'appel de Tunis a rendu un jugement en juin 2018, dont lequel elle a donné raison à l'INPDP, qui a considéré que des échantillons de sang collectés anonymement ne constituaient pas des données personnelles devant être protégées.

A noter, que depuis 2017, l'instance est de plus en plus sollicitée par les magistrats, les avocats et les huissiers notaires, autour de questions en relation avec la protection des données. D'un autre côté l'instance constate un intérêt porté à la question par les magistrats stagiaires au sein de l'Institut supérieur de la magistrature qui y consacrent leur mémoire de fin d'études.

En outre la justice administrative est interpellée de plus en plus sur des questions de protection des données personnelles. En avril 2019 le tribunal administratif de Tunis, a reçu une plainte contre une circulaire du ministre de l'éducation qui obligeait les enseignants présentant des demandes de congé de maladie, d'y adjoindre le certificat médical délivré par le médecin traitant. Le syndicat des enseignants jugeant cet acte illégal, introduisit un recours en annulation. Le Premier président du Tribunal administratif s'aligna aux arguments du requérant et accorda un sursis à exécution de la dite circulaire, en attente que le tribunal statue sur le fond.

Enfin, L'Instance provisoire de contrôle de la constitutionnalité des projets de lois, a été amenée à statuer sur un recours introduit par des députés contre un projet de loi sur le registre des entreprises, en arguant de l'inconstitutionnalité de son article 10. L'Instance rendit sa décision confirmant la violation du principe constitutionnel de protection des données personnelles.

III. Une diffusion de la culture de la protection dans la société

Les textes de loi ne peuvent à eux seuls faire le printemps. La protection des données personnelles est une question principalement de culture qu'il est impératif d'installer dans la société. La stratégie de l'INPDP dans ce cadre, depuis 2015, a donné ces fruits.

Les procédures préalables, les demandes d'avis et les plaintes devant l'INPDP ont totalisées au cours du premier mandat (2009 à 2011) 363 dossiers, ce chiffre a régressé au cours du deuxième mandat (2012-2014) avec 343 dossiers. Au cours du troisième mandat (2015-2017), ces chiffres ont été multipliés par huit, pour atteindre 2 663 dossiers. La tendance continue en 2018 et 2019, où l'INPD jusqu'au mois de mai 2019 a totalisé quelques 1 962 dossiers. La ventilation de ces dossiers démontre que les demandes d'avis et les plaintes sont en continuelle croissance.

L'Instance a fêté pour la première fois médiatiquement la Journée internationale en janvier 2019. Cela a été l'occasion de lancer un spot de sensibilisation télévisuel et radiophonique qui a été diffusé sur les médias nationaux et régionaux et repris par la presse. Elle a aussi organisé une conférence de presse le 28 janvier qui permis de faire le point sur la protection des données en Tunisie et dans le monde et ses perspectives. Cette action fut entreprise avec le soutien de l'Union Européenne dans le cadre du programme d'assistance amorcé en janvier 2019.

Malgré que la fonction de DPO ne soit pas prévu par la loi tunisienne, à ce jour, plus de 19 entreprises publiques et privées on en déjà nommé. L'Université Dauphine Tunis a même organisé en 2019 un Master de formation réservé à cette fonction et qui a eu un grand succès. L'INPDP a été invité à siéger dans le jury de soutenance des mémoires.

IV. Remise du premier rapport d'activité 2009-2017

L'Instance n'a jamais présenté depuis sa mise en place un rapport d'activité. A partir de 2015, le nouveau conseil de l'instance avait décidé de réaliser un rapport couvrant la période 2009-2017.

A l'occasion de la journée internationale de la protection des données personnelles, l'Instance présenta le rapport au président de la république, au président du Parlement et au chef du gouvernement. Il a été mis en ligne sur le site de l'Instance depuis janvier 2019 en langue arabe et au format audio. La version en langue française est en cours de traduction ainsi qu'un résumé mettant en exergue les tendances et les réalisations de ces neuf années d'activité.

V. Implication de l'INPDP dans les projets nationaux d'envergure

L'INPDP supervisa le projet d'inscription des élèves par le biais des téléphones portables pour la rentrée 2018. Elle a été également consultée lors de toutes les étapes de réalisation du projet d'installation des caméras de vidéo protection sur la voie publique. Elle a en outre collaboré avec la douane Tunisienne en vue de la mise en œuvre d'un projet pilote de recours aux caméras piétons portées par les agents.

L'INPDP a été invitée à présider la commission de pilotage du projet de mise en place du système national de déclaration de patrimoine par l'Instance nationale de lutte contre la corruption (INLUCC). Le lancement de la carte d'assurance maladie avait accusé un retard dans sa réalisation à cause des réserves émises par de l'INPDP, et n'a pu être amorcé qu'à partir de mars 2019, après que la caisse nationale d'assurance maladie se rallia aux points de vue de l'instance.

En avril 2018, le ministère de l'intérieur prenant en considération l'opposition de l'INPDP au projet de constitution d'une base de données biométriques systématique de la population en vue du lancement de la nouvelle carte d'identité, a proposé des solutions techniques répondant aux exigences de l'instance et permettant la préservation des données sensibles des citoyens. Le projet donnera lieu à un projet de loi concertée qui sera prochainement présenté au Parlement.

En octobre 2018, le projet du système SMS Stop mis en place par l'instance nationale des télécommunications à l'instigation de l'INPDP a été lancé au public avec un grand succès. Depuis, un SMS gratuit permet aux citoyens de bloquer toute réception des SMS publicitaires indésirables.

L'INPDP a permis l'adoption de la révision de la loi sur la pratique médicale, en y insérant des dispositions protectrices des données personnelles dans le cadre de l'exercice de la télémédecine.

VI. Amorce des missions de contrôle in situ des responsables de traitement

Dans le cadre du développement de son activité tendant à rehausser le niveau de protection des données personnelles, l'INPDP a élaboré un projet de programme de contrôle des organismes publics et privés, traitant des données personnelles. Il est prévu que ce programme soit mis à exécution à partir de juillet 2019. Cette action a été rendue possible grâce au soutien du Conseil de l'Europe et l'assistance de l'EDPS. Une formation des membres de l'Instance se tiendra à Tunis les 17 et 18 juin 2019. Les premières opérations de contrôle in situ sont programmés à partir de juillet.

VII. L'INPDP sur le plan international

L'INPDP a développé sa présence sur le plan international. C'est ainsi que son Président a été désigné Président par intérim de l'Association francophone des autorités de protection (AFAPDP).

L'Instance a été aussi nommé membre du comité de préparation du programme de la session ouverte de la conférence internationale de 2019 qui se tiendra à Tirana en octobre.

Enfin, l'INPDP a entrepris un lobbying politique qui permis à l'Etat tunisien, le 24 mai 2019, de devenir le trentième signataire de la 108+ et son deuxième Etat non européen. Un projet de loi de ratification du protocole a été proposé au Chef du Gouvernement début juin 2019.

EUROPEAN COMMISSION/ COMMISSION EUROPENNE

Input from the European Commission (Directorate-General for Justice and Consumers, Unit C4 – International Data Flows and Protection)

A pivotal year for data protection and privacy, both in the EU and globally

The General Data Protection Regulation **("GDPR")** entered into application on 25 May 2018. The regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. The single law also puts an end to the fragmentation between different national systems and unnecessary administrative burden.

The Data Protection Directive for Police and Criminal Justice Authorities **("Police Directive")** entered into force on 5 May 2016 and EU Member States had to transpose it into their national law by 6 May 2018. The directive protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes. It ensures that the personal data of victims, witnesses, and suspects of crime are duly protected and facilitates cross-border cooperation in the fight against crime and terrorism.

The European Commission set out its approach to the application of GDPR in its Communication on "Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018", of 24 January 2018 and its Communication on "Completing a trusted Digital Single Market for all" of 15 May 2018. In particular, the European Commission called on Member States to carry out all the necessary actions in a timely manner and to equip the data protection authorities with sufficient resources.

In September 2018, the European Commission issued an electoral package including data protection guidance in the electoral context.

To support SMEs in their efforts to comply with the GDPR, the Commission developed an online toolkit with 60 questions and answers on the GDPR, as well as dedicated brochures. Moreover, the Commission allocated several sets of grants to support awareness-raising actions by Data Protection Authorities in particular towards SMEs. Such actions include the setting up of hotlines and the drafting of practical compliance tools.

Following broad public consultations, the **European Data Protection Board** (previously known as 'Article 29 Working Party') has adopted detailed guidelines on novel aspects of the GDPR, for example on the use of the so-called derogations for specific situations in the area of international transfers. All adopted guidelines are available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

This work will continue in the coming months, showing that compliance is a dynamic process characterised by a close dialogue between regulators and stakeholders. The European Commission actively contributes to the work of the European Data Protection Board whose guidelines are of key importance to help stakeholders implement the GDPR.

International dimension of the GDPR and global convergence

The entering into effect of the European Union's modernised data protection rules has triggered **similar reforms** in its neighbourhood, from Georgia to Switzerland to Tunisia. A growing number of countries around the world[8], from Chile to Japan, from Brazil to India, from Argentina to Indonesia, and from Tunisia to Kenya, are updating or adopting new privacy laws that tend to be based on common elements, which they share with European rules.

These laws converge on the model of a modern data protection law that combines at least four essential features: (1) an overarching legislation applicable across all sectors, (2) a core set of data protection principles and obligations, (3) enforceable individual rights, and (4) enforcement by an independent supervisory authority.

This developing **convergence in privacy standards at international level** offers new opportunities to facilitate data flows and thus trade, while improving the level of protection of personal data when transferred abroad. The recently concluded **arrangement between the EU and Japan** illustrates this point: in January 2019, both sides adopted mutual adequacy findings. Together, these adequacy findings create the world's largest area of free and safe data flows, thus benefitting thousands of companies on both sides.

With regard to transatlantic flows of personal data, the **EU-US Privacy Shield** adopted in 2016 was subject to its **second annual review** in October 2018. The European Commission adopted its report to the European Parliament and the Council on 19 December 2018, noting that several aspects of the practical functioning of the Privacy Shield have improved and concluding that the Privacy Shield continues to provide an adequate level of data protection.

Other important positive developments in recent months on the international front include:

- the conclusion of the negotiations on **Passengers Name Record (PNR) with Canada**, providing for strong safeguards that guarantee the fundamental rights of our citizens;

- the development of a **multilateral Administrative** between the International Organization of Securities Commissions (IOSCO) and the European Securities and Markets Authority (ESMA) for the cooperation of financial supervisors. The Arrangement will allow for the continued exchange of enforcement and supervisory information between securities regulators in order to promote orderly markets and protect

[8] In Asia, the Indian Supreme Court recently recognised data protection as a fundamental right, and the government has since then drafted a strong data protection bill. Indonesia is also advanced in its preparations and should soon start discussions in parliament. Thailand recently adopted a modern data protection law. Japan reformed – and significantly strengthened its rules – in 2017. Korea, which already has strong rules and enforcement, is further strengthening its law and intends to significantly expand the powers of its general data protection authority. In Latin America, Argentina is in the process of amending its existing data protection law. Brazil recently adopted a brand new law and is currently discussing the one remaining, but crucial element, the creation of an independent data protection authority. Colombia is considering updating its law. Mexico for some time already has strong data protection rules, and played a fundamental role in drafting the Ibero American Data Protection Standards as a model rulebook for data protection in the region. Uruguay has recently amended its data protection framework by introducing key accountability elements such as the position of DPO and data breach notification. One important country absent from this list so far is the US, which at Federal level currently only has sectoral rules. However, a serious debate has started in the US on whether to create a horizontal, federal law.

investors, while providing safeguards for the protection of personal data. The European Data Protection Board issued a positive opinion on the Arrangement.

First lessons from 1-year of GDPR application

The European Commission will take stock of one year of application of the GDPR in an event on 13 June. As foreseen by the GDPR, the Commission will report on the application of the new rules in 2020.

Among the first lessons that can be drawn from 1-year of GDPR application, the European Commission highlights the following:

- For companies, compliance with the GDPR has proven to be first of all an opportunity to put their data house in order by taking a closer look at what data they are collecting, what they use it for, how they keep and share it, and, not the least, whether they really need to collect and process all this data. Answering these questions has often allowed business to reduce exposure to unnecessary risks but also to get a better idea of what data they hold and develop a more trustworthy relationship with their customer and commercial partners.

- The citizens also took advantage of the GDPR. They have exercised their data protection rights with controllers, and they have also used their right to submit complaints to data protection authorities. There has been an increase in the number of complaints received by Data Protection Authorities since the entry into application of GDPR (amounting to an overall of about 95.000 complaints across the EU at the end of January 2019). NGOs active in the field of data protection have also started to make use of the possibility to bring representative actions before data protection authorities and courts (e.g. the French DPA (CNIL) issued on 21 January 2019 a fine of 50 million euros against Google in relation to two collective complaints filed by NOYB and La Quadrature du Net about the conditions for obtaining consent).

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

In the EDPS Strategy 2015-2019, we outline a vision of an EU that leads by example in the global dialogue on data protection and privacy in the digital age. We set ourselves a challenging and ambitious agenda, which we have sought to carry out over the course of the current mandate.

We made great strides towards achieving these goals in 2018, a year which could be considered pivotal both in the history of data protection and in the history of the EDPS.

New legislation for a new era

One of the three objectives set out in our Strategy was to open a new chapter for EU data protection. Technological development is moving at a rapid pace and the way in which we live, as individuals and as a society, is also changing rapidly to accommodate this. Logically, the EU's data protection rules also required an update, not aimed at slowing down innovation, but at ensuring that individuals' fundamental rights are protected in the digital era.

On 25 May 2018, new data protection legislation became fully applicable to all companies and organisations operating in the EU Member States. The General Data Protection Regulation (GDPR) marked the first step towards ensuring comprehensive and effective protection of personal data and privacy for all individuals in the EU.

With this new legislation came the establishment of the European Data Protection Board (EDPB). Made up of the 28 EU Member State data protection authorities (DPAs) and the EDPS, this new body is entrusted with ensuring the consistent implementation of the GDPR across the EU. Charged with providing the secretariat for this new EU body, a significant amount of our time and effort in early 2018 went into ensuring that the Board would be prepared to deal with its heavy workload from day one of the new Regulation. We have continued to support the EDPB secretariat administratively throughout the year, as well as participating fully as a member of the Board itself.

We moved yet another step closer to achieving a comprehensive framework for data protection with the adoption of new rules for the EU institutions and bodies. Regulation 2018/1725 came into force on 11 December 2018, bringing the rules for the EU institutions in line with the rules set out in the GDPR.

As the supervisory authority for data protection in the EU institutions and bodies, we faced the significant challenge of ensuring that they were all prepared for these new rules. In 2017, we embarked on a campaign of visits, training sessions and meetings, which intensified over the course of 2018. These were aimed at raising awareness and about the new rules and helping to ensure that the EU institutions had the knowledge and tools to put them into practice.

A specific focus of these activities was on encouraging the development of a culture of accountability within the EU institutions. We wanted to ensure that they not only comply with data protection rules, but that they can demonstrate this compliance. Integral to this was creating awareness that the processing of personal data, even when done lawfully, can put the rights and freedoms of individuals at risk. These activities will continue into 2019, as we endeavour to ensure that the EU institutions lead the way in the application of new data protection rules.

The misuse of personal data for tracking and profiling purposes and the role of technology in our society was a topic of significant public debate in 2018. The EDPS and the data protection community in general were at the forefront of this debate, with the EDPS contributing on two main fronts: through our Opinion on online manipulation and personal data and our Opinion on Privacy by Design.

While the former focused on the need to extend the scope of protection afforded to individuals' interests in today's digital society, the latter looked to address the new challenges resulting from technological and legal developments. On the legal side, the new generation of data protection rules laid down in the GDPR, Directive 2016/680 and Regulation 2018/1725 on the processing of personal data by EU institutions requires that controllers take account of the state of the art in technical and organisational measures to implement data protection principles and safeguards. This also requires that supervisory authorities are aware of the state of the art in this domain and that they follow its development. Cooperation in this field is of crucial importance in order to ensure that these principles are applied consistently. The Opinion also built on our work with the Internet Privacy Engineering Network (IPEN) to encourage dialogue between policymakers, regulators, industry, academia and civil society on how new technologies can be designed to benefit the individual and society.

The new data protection rules also introduce the principle of accountability. All controllers, including the EU institutions and bodies, must ensure that they are able to demonstrate compliance with the new rules. This also applies to the management and governance of their IT infrastructure and systems. To help with this, we extended our catalogue of specific guidelines to include, among others, Guidelines on the use of cloud computing services by the EU administration and further guidance on IT management and IT governance. In 2018, we also began a systematic programme aimed at verifying EU bodies' compliance with EDPS guidelines.

Finding a balance between security and privacy

1 May 2018 marked one year since the EDPS took over responsibility for supervising the processing of personal data for operational activities at the EU's law enforcement agency, Europol. One of the action points set out in our Strategy as integral to opening a new chapter for data protection in the EU is to promote a mature conversation on security and privacy. As an EU agency charged with ensuring the security of the EU while protecting the fundamental rights to privacy and data protection, Europol is a great example of the progress we are making in this area.

We continue to maintain a strong relationship with Europol's Data Protection Officer (DPO) and Data Protection Function (DPF) Unit, which allows us to ensure that we are able to anticipate any possible problems and plan future activities. We carried out our second inspection of data processing activities at the agency in May 2018 and continued to provide advice and deal with complaints where required.

The security of EU borders remains a hot topic and the EU legislator put forward several new proposals in 2018 aimed at increasing security and improving border management. While we recognise the need for greater EU security, this should not come at the expense of data protection and privacy.

Facilitating responsible and informed policymaking is another of the action points required in order to open a new chapter in EU data protection. With this in mind we issued several Opinions on proposed EU border policy in 2018. One of these focused on the future of information sharing in the EU, addressing Proposals for two Regulations which would establish a framework for interoperability between EU large-scale information systems. As the implications of this Proposal for data protection and other fundamental rights

and freedoms are uncertain, we will launch a debate on this issue in early 2019 to ensure they are explored in detail.

We also continued our close cooperation with DPAs to ensure effective and coordinated supervision of the EU's large-scale IT databases, used to support EU policies on asylum, border management, police cooperation and migration.

Developing partnerships

Facilitating responsible and informed policymaking is far from limited to the field of EU security and border policy, however. In 2018, the EDPS issued 11 Opinions, including two upon request from the Council, on matters ranging from jurisdiction in matrimonial matters to the interoperability of EU large-scale information systems.

We also issued 14 sets of formal comments. These are equivalent to Opinions, but typically shorter and more technical. Some of our comments were expressly requested by the European Parliament, or one of its Committees, and concerned not the initial legislative proposals, but draft amendments and outcomes of negotiations between the co-legislators.

Taking into account that we also dealt with over 30 informal consultations on draft proposals by the Commission, these numbers clearly demonstrate the increased need for, and relevance of, independent expert advice on the data protection implications of EU initiatives, as well as growing interest from EU institutional stakeholders. We look forward to continuing this mutually beneficial cooperation in the coming years in the context of strengthened legislative consultation powers under the new Regulation 2018/1725.

We also continued our efforts to ensure that activities within the EU institutions are carried out in accordance with the relevant data protection laws, issuing prior-check Opinions, investigating complaints and monitoring compliance through the various tools available to us.

The Strategy commits the EDPS to forging partnerships in pursuit of greater data protection convergence globally. While data flows internationally, across borders, data protection rules are decided on a largely national, and at best regional, basis.

With this in mind, we continue to work with our regional and international partners to mainstream data protection into international agreements and ensure consistent protection of personal data worldwide.

We are also involved in discussions on adequacy findings. These agreements are made by the European Commission on behalf of the EU Member States, and provide for the transfer of data from EU countries to non-EU countries whose data protection rules are deemed to provide adequate protection. Specifically, in 2018, we contributed to the second joint review of the EU-US Privacy Shield and to the EDPB Opinion on a proposed adequacy agreement with Japan.

Digital Ethics and the International Conference

We launched the EDPS Ethics Initiative back in 2015, as part of our commitment to forging global partnerships. We wanted to generate a global discussion on how our fundamental rights and values can be upheld in the digital era.

Three years on and digital ethics is now very much on the international agenda.

We began 2018 with the publication of the Ethics Advisory Group Report. The Report is a useful tool in helping us to understand how the digital revolution has changed the way we live our lives, both as individuals and as a society. It also outlines the changes and challenges this implies for data protection. From here, we were able to expand our enquiry to reach a much larger audience, through a public consultation launched in early summer 2018. The results of the consultation revealed the importance of ethics moving forward and called for DPAs to play a proactive role in this.

However, it was the International Conference of Data Protection and Privacy Commissioners, dubbed the *Olympic Games of Data Protection* by EDPS Giovanni Buttarelli, that really launched the discussion on digital ethics onto the international agenda.

The public session of the International Conference focused on *Debating Ethics: Dignity and Respect in Data Driven Life*. With over 1000 people from a variety of different backgrounds, nationalities and professions in attendance, high-profile speakers and considerable media coverage, the event served to foster debate on the issue and put new ethical and legal questions high on the agenda of DPAs and others across the world. The EDPS is now seen as a leader in this area and will work hard to progress the debate.

Internal administration

With our role and responsibilities expanding, good internal administration has been more important than ever in ensuring that we are able to achieve our goals.

The EDPS Human Resources, Budget and Administration (HRBA) Unit tackled two particularly big preparatory tasks in 2018. Work on preparations for the new **EDPB secretariat** intensified significantly in order to ensure that the Board was administratively and logistically prepared to start work on 25 May 2018. Among other things, this involved ensuring that all EDPB staff members were subject to the same rules as those working for the EDPS and able to benefit from the same rights.

Ahead of the new data protection Regulation for the EU institutions, we also had to ensure that all EDPS HR decisions complied with the new rules. We therefore undertook a full review of all EDPS HR data processing activities and revised our approach as needed.

In addition to a number of initiatives aimed at improving our HR policies, we launched a new open competition to create a pool of highly qualified data protection experts to satisfy our future recruitment needs. As we move into 2019, our main aim is to ensure an efficient and pleasant work environment for all those who work at the EDPS.

AEDH

GREECE

Major developments in the data protection field in Greece since June 2018

- Greece has not yet adopted a new Data Protection Act. A draft act went trough public consultation in February 2018, but the final version has not yet brought to Parliament.
- The Hellenic DPA published the list of types of processing for which the data controller must carry out a DPIA (decision 65/2018).
- A call for recruitment for new staff was launched by the DPA. The procedure is still ongoing.
- The DPA organised trainings on data protection and the GDPR for the Public sector in cooperation with the National School of Public Administration and for the Health sector in cooperation with the Center for European Constitutional Law, the Laboratory of Legal Informatics of the University of Athens, the Office of the Commissioner for Personal Data Protection of Cyprus and the University of Cyprus.
- The DPA carried out an ex-officio action with the aim of (a) investigating the level of compliance with the GDPR and the e-Privacy legislation (b) raising awareness among data controllers and data subjects. A total of 65 data controllers, active online in the financial services, insurance, e-commerce, ticketing and public sector services, were tested to meet specific requirements in the fields of transparency, the use of cookies, the sending of e-mails and the security of websites through indicative control points, perceived by the citizen when navigating the internet and using the Internet n services. The initial conclusions resulting from this action were the following:
    - Lack of compliance with the legislation on cookies and related technologies, to almost all controllers.
    - Lack of information on processing operations and recipients of data in about 40% of the controllers. Compliance of the Public sector especially in the area of transparency was problematic.
    - On the contrary, a high level of over 80% of data controllers showed a satisfactory basic safety level.

○ In addition, there was an adequate degree of disclosure of data protection officer in the private sector, in excess of 70% of the controllers.

LUXEMBOURG

RGPD

Le 26 juillet 2018 la Chambre des députés a adopté deux projets de loi sur la protection des données, les projets de loi n°7184 et n°7168 complètent le règlement général sur la protection des données (RGPD).

Projet de loi n° 7184: organisation de la CNPD et mise en oeuvre du RGPD

Le projet de loi concerne la création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Son objectif était d'adapter le droit luxembourgeois au nouveau cadre européen pour en assurer la pleine effectivité pour les citoyens et les responsables de traitement et sous-traitants.

Le projet de loi est devenu la Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données

Projet de loi n°7168: protection des données en matière pénale ainsi qu'en matière de sécurité nationale

Le deuxième projet de loi adopté est relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Il est censé transposer la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Après l'entrée en vigueur du règlement général sur la protection des données du 25 mai 2018, la CNPD du Luxembourg (Commission nationale pour la protection des données) s'est fixée l'objectif de mettre en œuvre des mécanismes de certification en matière de protection des données. A cet effet, la CNPD a lancé une consultation publique concernant son schéma de certification de traitements de données à caractère personnel « GDPR Certified Assurance Report based Processing Activities (GDPR-CARPA)».

Lignes directrices en matière de vidéosurveillance

Le 14 août 2018 la CNPD a publié des lignes directrices en matière de vidéosurveillance. En effet, suite à l'entrée en application du RGPD, la CNPD a souhaité rappeler certains principes et certaines obligations applicables en la matière. Elles s'adressent aux responsables du traitement souhaitant avoir ou ayant recours à des dispositifs de vidéosurveillance.

Le 28 septembre 2018 la CNPD a rapporté les premiers retours d'expérience concernant les violations de données. Premiers retours d'expérience concernant les violations de données

Lignes directrices concernant « les campagnes électorales dans le respect de la protection des données personnelles ».

Le 19 avril 2019 la CNPD a publié des lignes directrices en vue des élections européennes qui ont eu lieu le 26 mai 2019. A la lumière des révélations de *Cambridge Analytica* et des controverses autour des phénomènes de la désinformation et de la manipulation, la CNPD a souhaité sensibiliser les acteurs politiques sur les risques liés en particulier à la collecte et au traitement des données à caractère personnel des électeurs à des fins électorales.

discours de haine sur les réseaux sociaux

Concernant la lutte contre les discours de haine sur les réseaux sociaux il existe depuis longtemps l'initiative BEE SECURE qui en cas de dérapage n'hésite pas à porter plainte.

BEE SECURE est une initiative commune du Ministère de l'Economie, du Ministère de la Famille, de l'Intégration et à la Grande Région et du Ministère de l'Education nationale, de l'Enfance et de la Jeunesse.

Un « memorandum of understanding » a été signé en 2008, par les ministres en charge de l'éducation nationale, de l'enfance et de la jeunesse, de l'économie et de la famille et fut la base de l'initiative BEE SECURE. Ce memorandum fixe une approche commune et coordonnée d'actions de sensibilisation et de formation. Ce memorandum et les actions en ressortant sont repris dans le cadre de la « Cyber Security Strategy III », publiée par le gouvernement en mai 2018.

L'initiative BEE SECURE englobe les actions au niveau de la sensibilisation à une utilisation plus sécurisée des technologies de l'information et de la communication.

BEE SECURE est aussi un projet financé en partie par la Commission Européenne, et qui fait fonction de centre de sensibilisation luxembourgeois au sein du réseau paneuropéen Insafe.

PORTUGAL

GDPR

General remarks: The Portuguese National Data Protection Committee (CNPD) continues to have very little resources (financial and human) to cope with this big responsibility and supervision specially after the GDPR.

In terms of legislation, the national dispositions contained in the GDPR are yet to be adopted by the Portuguese Parliament, with its conclusion and final vote expected to take place in June 2019.

The Portuguese National Data Protection Committee (CNPD) issued 2 Guidelines: 1 on Data made available online by schools regarding students (October 2nd 2018); and another one on Personal Data in the context of political campaigning and political marketing (March, 25th, 2019).

4 fines were issued by the CNPD since June 2018 until June 2019:

October, 9th, 2018: Issued fine of 400,000.00 € (four hundred thousand euros) on a Public Hospital for failing to comply with the number 3 of article 83º of the GDPR. The data of patients was found to be accessed without enough controls and almost freely by any worker at the hospital (number of accesses was also found to be higher than the number of workers).

February, 5th 2019: Issued fine of 20,000.00€ (twenty thousand euros) on a Call Center for having destroyed a phone call with a data holder and for preventing to give him access to the copies or transcripts of telephone calls.

March, 19th, 2019: Issued fine of 2,000.00€ (two thousand euros) on a business owner for operating 9 video cameras and 1 recorder without any sign/information stating it had these systems. This was detected in an inspection by the Police.

March, 25th, 2019: Issued fine of 2,000.00€ (two thousand euros) on a business owner for operating video cameras without any sign/information stating it had these systems. This was detected in an inspection by the Police."

FRANCE

MISE EN ŒUVRE DU RGPD

La loi dite « Informatique et Libertés » de 1978 (dont la CNIL a célébré les 40 ans en 2018) a été refondue pour permettre une pleine application du RGPD et aménager les marges de manœuvre nationales (loi n° 2018-493 du 20 juin 2018). Cette loi a également permis de transposer la directive Police Justice

Le récent décret, publié le 30 mai 2019, a constitué la dernière étape de la mise en conformité du droit national avec le Règlement général sur la protection des données (RGPD) et la Directive « police-justice », applicable aux fichiers de la sphère pénale. Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

La CNIL a émis un avis très critique sur ce décret :
https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038530105

SANCTIONS

Exemple de sanction infligée par la Commission nationale informatique et libertés :

Juin 2019 : la CNIL a infligé une amende de 400.000 euros à une société immobilière, Sergic, qui avait laissé accessibles en ligne des informations personnelles de candidats à la location. Cette société immobilière située dans le Nord a des activités de gestionnaire d'immobilier, de syndic de co-propriété, de location de vacances, et d'immobilier d'entreprise.société.

Dans un contrôle en ligne le 7 septembre, la Cnil a constaté que des copies de cartes d'identité, carte Vitale, jugement de divorce, attestations de la Caisse d'Allocations Familiales étaient accessibles "sans authentification préalable".

Dans un contrôle sur place quelques jours plus tard, elle s'est également rendue compte que l'entreprise connaissait la vulnérabilité "depuis mars 2018", mais avait attendu le 17 septembre 2018 pour la corriger. De plus ces données étaient conservées sans limitation de durée.

LOI RELATIVE À LA LUTTE CONTRE LA MANIPULATION DE L'INFORMATION

La loi organique n° 2018-1201 relative à la lutte contre la manipulation de l'information a été promulguée le 22 décembre 2018. Elle impose de nouvelles obligations de transparence aux opérateurs de plateforme sur les « contenus d'information se rattachant à un débat d'intérêt général », pendant les trois mois avant une élection importante : présidentielle, législatives, européennes, etc. Les plateformes devront par exemple révéler aux utilisateurs « une information loyale, claire et transparente » sur l'identité de ceux qui ont payé pour promouvoir « des contenus d'information se rattachant à un débat d'intérêt général ». Une infraction à ces dispositions sera passible d'un an de prison et de 75 000 euros d'amende.

PROPOSITION DE LOI VISANT À LUTTER CONTRE LA HAINE SUR INTERNET

Une proposition de loi portée par la députée Laetitia Avia a été déposée à l'Assemblée nationale le 20 mars 2019. Elle vise à obliger les plateformes dépassant un certain seuil mensuel de connexions (déterminé par décret ultérieurement) à une série d'obligations, notamment l'obligation de retrait en 24 heures des contenus manifestement « haineux » qui leur auront été signalés. Elle devrait permettre d'intervenir plus efficacement contre les propos haineux sur internet. Toutefois la loi ne s'attaque pas aux auteurs de ces propos, et de nombreuses limites à son efficacité ont été relevées. Le Conseil d'État a publié un avis plutôt critique et le Projet sera donc modifié avant examen en juillet à l'Assemblée nationale.

FICHIERS

FICHAGE DES MINEURS ÉTRANGERS ISOLES

Le décret n° 2019-57 du 30 janvier 2019 réformant les modalités d'évaluations des **étrangers se déclarant mineurs isolés** porte la création d'un fichier biométrique de ces personnes (dénommé AEM pour Appui à l'Évaluation de la Minorité). Sous prétexte de lutte contre la fraude le décret prévoit d'enregistrer dans le fichier AEM les empreintes digitales et la photo numérisée.

Ce décret a été attaqué en Conseil d'État par des associations de défense des droits de l'Homme, mais aussi des organisations de protection de l'enfance et même par l'UNICEF[9].

COUPLAGE DES FICHIERS HOPSYWEB ET FSPRT

Un décret publié au Journal officiel du 8 mai 2019 (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038442383&categorieLien=id) permet de coupler le fichier de suivi des personnes en soins psychiatriques sans consentement (HOPSYWEB) avec celui relatif aux signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT). Les données de patients hospitalisés en psychiatrie pourront désormais, grâce aux dispositions du décret être comparées au fichier des radicalisations. Ce croisement entre les données enregistrées dans les 2 fichiers sera réalisé, a minima toutes les 24h00.

La CNIL a critiqué ce décret (https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038442727), elle estime que la possibilité d'introduire une dérogation au secret professionnel permettrait, en particulier aux nombreux agents des préfectures accédant au FSPRT, d'être destinataires d'informations couvertes par le secret médical. En outre le décret ne prévoit pas d'informer les personnes hospitalisées de la nouvelle finalité du fichier.

De nombreuses informations relatives aux changements majeurs sur la protection des données sont publiées sur le site NexInpact (https://www.nextinpact.com/)

- 9QPC présentée par Spinosi & Sureau déposée par le Groupe d'information et de soutien des immigré.e.s (GISTI) : https://www.gisti.org/IMG/pdf/req_unicef-et-autres_qpc-decret_2019-01-30.pdf
- Dépôt du référé en suspension par Spinosi & Sureau par le GISTI : https://www.gisti.org/IMG/pdf/req_unicef-et-autres_rs_decret_2019-01-30.pdf
- Dépôt du recours pour excès de pouvoir par Spinosi & Sureau par le GISTI: https://www.gisti.org/IMG/pdf/req_unicef-et-autres_rep_decret_2019-01-30.pdf

UKRAINE / UKRAINE

The Action Plan for the implementation of the Association Agreement between Ukraine and the EU was adopted on October 25, 2017, by the Resolution of the Cabinet of Ministers of Ukraine No. 1106.

The requirements for amending the legislation on data protection with the purpose to bring it into line with the General Data Protection Regulation of the EU were stipulated by the paragraph 11 of the Action Plan. There are steps to accomplish this task, in particular, drafting of a law on amending the Law of Ukraine «On Personal Data Protection». The Ukrainian Parliament Commissioner for Human Rights (consensual), the Ministry of Justice of Ukraine, the Ministry of Finance of Ukraine, the Ministry of Economic Development and Trade of Ukraine and the Ministry of Internal Affairs of Ukraine are defined responsible for implementing of the paragraph 11 of the Action Plan.

Also, the Coordination Council for the improvement legislation in the field of data protection was established in the Secretariat of the Commissioner, which includes representatives of Executive power bodies of Ukraine, other state bodies, parliamentary groups and factions in the Parliament of Ukraine, as well as public representatives.

Additionally, with aim of strengthening the effectiveness of the Secretariat of the Commissioner by improving the legislation in the field of the human rights protection and activities of the Ombudsman, establishing practice in applying this legislation, as well as bringing the institutional framework of the Ombudsman Office and its internal procedures in compliance with the international and European best practices realizing Twinning Project «Implementation of the best European practices to strengthen institutional capacity of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights to protect human rights and freedoms (Secretariat)», that is aimed at, among other things, improvement on the provision of rights in the field of data protection.

The Coordination Council, together with the Lithuanian and Austrian experts of the Twinning Project, has drawn up new draft of the Law «On Personal Data Protection», taking into account the main innovations of GDPR. This draft foresees gradual approximation with EU legislation.

Also, this draft was often discussed at working meetings and round tables held in the Secretariat of the Commissioner.

At the same time, during the work on the draft the number of controversial norms was revealed. For example, the norm on increasing the effectiveness of investigating human rights violations, that the Commissioner's de facto allocation of investigative functions. Other norms regarding the Commissioner's ability to impose penalties for violations in the area of personal data protection directly are under discussion. There are some reservations on these issues (including the Ministry of Justice of Ukraine). This «punitive» function is not inherent in the legal nature of the Ombudsman, whose priority is the protection and restoration of violated rights of citizens through various legal methods, in particular, with the application of reconciliation procedures, legislative initiatives, etc.

Today, in the field of personal data protection, the Commissioner is empowered to draw up Protocols on administrative offenses and send them to courts in cases stipulated by law. Courts have the right to impose fines.

It should be noted that the function of exercising parliamentary control over the observance of constitutional human and citizens' rights and freedoms is performed by the Commissioner according to the Law of Ukraine «On the Ukrainian Parliament Commissioner for Human Rights». This function does not coincide with giving the Ombudsman such authority as the penalization and some other powers, for example, carrying out investigative functions.

Whether there should be created a new data protection authority is currently under discussion.

I would like to draw your attention to the fact that we already had a separate body for the protection of personal data – the State Service of Ukraine on Personal Data Protection. Its activities were directed and coordinated by the Cabinet of Ministers of Ukraine through the Minister of Justice of Ukraine.

At the same time, in order to ensure the independence of the personal data protection authority, as required by the Council of Europe Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data No. 108, the State Service was abolished in 2014. And according to the amendments to the Law of Ukraine «On Personal Data Protection» the function of control over observance of the legislation on protection of personal data is assigned to the Commissioner.

The 20th Central and Eastern Europe Data Protection Authorities Meeting was held in Ombudsman Office in 2018, where Data Protection Authorities representatives discussed the implementation of international standards for data protection, and the implementation of the provisions of the General Data Protection.

The conference was attended by representatives of Lithuania, Georgia, Bosnia and Herzegovina, Croatia, Hungary, Montenegro, Serbia and Ukraine. The representatives discussed the implementation of international data protection standards, in particular, the implementation of the General Regulations on Data Protection in national legislation, as well as the issue of signing a protocol amending the Council of Europe Convention “On the Protection of Persons in connection with the automated processing of personal data”.

The Office of the Commissioner actively analyzes experience in the field of personal data of EU countries, countries of Eastern Europe and the United States.

URUGUAY

In the past year Uruguay decided to update it´s legislation, acknowledging the newest developments in the field of protection of personal data in the world -reflected in the modernization of Convention 108 and the GDPR-, and considering the guidelines provided by the Standards on Data Protection issued by the Iberoamerican Network on Data Protection.

It should be noted that uruguayan law (N° 18.331, enacted on 11th. august, 2008) was already a modern legislation, so few adaptation were needed to update its provisions. These changes, which were established by articles 37 to 40 of Law No. 19.670, effective as of January 1, 2019, are as follows:

- **Extraterritoriality**: The scope of application of Law 18.331 is extended, giving the URCDP jurisdiction outside the national territory when: a) data of inhabitants of Uruguay are processed for the offering of goods or services, or for the analysis of their behavior; b) determined by contracts or international instruments; c) means located in the country are used.
- **Data breaches**: Imposes controllers and processors the obligation of informing immediately data subjects and the URCDP whenever a data breach is detected. Controllers and processors should also inform the measures adopted to correct such breaches.
- **Accountability Principle**: Controllers and processors are obliged to ensure compliance with the provisions of the law, by adopting the appropriate technical and organizational measures. They should also give proof of compliance when required by the URCDP.
- **Data Protection Delegate**: Private entities that process sensitive data as their main activity and those who process large volumes of data, as well as public entities in general must incorporate the role of the "Data Protection Delegate" in their organizations. This Data Protection Delegate will be in charge of advising, proposing and supervising personal data protection policies.

The URCDP is nowadays working on generating a more detailed regulation based on such provisions, that expects to be approved in the course of the present year.

In addition to the usual activities with public entities in general and the annual contests organized jointly with the public schooling authorities, the URCDP specifically addressed the issue of protection of personal data in local governments, generating a network of contacts and data protection delegates to foster compliance with the law.

Finally, as part of the URCDP´s policy of extending the knowledge on data protection amongst processors, controllers and public in general, three guides were published on the topics of cookies, byod and drones. These guides, as well as all the information regarding the activities of the URCDP are available through the webpage: www.datospersonales.gub.uy.