



Strasbourg, 21 June / juin 2021

T-PD(2021)Mos

**CONSULTATIVE COMMITTEE 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 récents 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

| | |
|--|----|
| ALBANIA / ALBANIE | 4 |
| ARGENTINA / ARGENTINE..... | 8 |
| AUSTRIA / AUTRICHE..... | 9 |
| BOSNIA AND HERZEGOVINA / BOSNIE ET HERZÉGOVINE | 10 |
| CAPE VERDE / CAP VERT | 15 |
| CROATIA / CROATIE..... | 17 |
| CYPRUS / CHYPRE..... | 20 |
| CZECH REPUBLIC / REPUBLIQUE TCHEQUE | 21 |
| EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) / LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD) | 22 |
| ESTONIA / ESTONIE | 26 |
| FINLAND / FINLANDE | 28 |
| FRANCE | 29 |
| GEORGIA / GEORGIE | 33 |
| HUNGARY / HONGRIE..... | 40 |
| INDONESIA / INDONÉSIE | 42 |
| ITALY / ITALIE..... | 43 |
| INTER-AMERICAN INSTITUTE OF HUMAN RIGHTS (IHR) / INSTITUT INTER-AMERICAIN DES DROITS DE L'HOMME | 48 |
| JAPAN / JAPON | 49 |
| INTERNATIONAL COMMITTEE OF THE RED CROSS / COMITÉ INTERNATIONAL DE LA CROIX- ROUGE (ICRC) | 51 |
| LIECHTENSTEIN | 53 |
| MALTA / MALTE..... | 54 |
| MAURITIUS / MAURICE | 55 |
| MEXICO..... | 56 |
| MOLDOVA..... | 57 |
| NORTH MACEDONIA / MACÉDOINE DU NORD | 59 |
| MONTENEGRO / MONTÉNÉGRO | 60 |
| MONACO..... | 61 |

| | |
|---|----|
| PORTUGAL | 64 |
| SAN MARINO / SAINT-MARIN | 65 |
| SERBIA/ SERBIE | 66 |
| SLOVAK REPUBLIC / RÉPUBLIQUE SLOVAQUE | 68 |
| SLOVENIA / SLOVENIE..... | 69 |
| SWEDEN / SUÈDE | 71 |
| SWITZERLAND / SUISSE..... | 72 |
| TURKEY / TURQUIE | 74 |
| UKRAINE..... | 76 |
| UNITED KINGDOM – OVERSEAS TERRITORIES / ROYAUME-UNI – TERRITOIRES D’OUTRE-MER | 79 |
| URUGUAY..... | 81 |

ALBANIA / ALBANIE

Information and Data Protection Commissioner (IDP) *(Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale)*

REPORTING PERIOD (NOVEMBER 2020 – 4 JUNE 2021)

Public awareness

National campaign on digital education: “Play and learn – Happy Onlife”

The national campaign on digital education “Play and learn – Happy Onlife” is an awareness-raising initiative by the Information and Data Protection Commissioner’s Office related to the safe use of the digital environment by children. In the course of October – December 2020, and May 2021, (due to and in respect of preventive/restrictive measures in Albania in relation to the global pandemic COVID-19) 31 meetings were held with 9-year schools in the following cities: Kavaja, Rrogozhina, Cërrik, Gramsh, Belsh, Peqin, Elbasan, Librazhd, Laçi, Kruja, Rrëshen, Lezha, Shkodra, Koplik, Kukës Krumë, Burrel, Klos, Vora, Kamza and Durrës. Representatives of the Commissioner’s Office shared information and practical advices on privacy protection with pupils and teachers, particularly on the use of social networks. The “Happy Onlife” game aims at encouraging critical thinking of youngsters in order to raise their awareness and build knowledge on internet safety.

28-th January – Personal Data Protection Day and the 40th anniversary of the Council of Europe’s Convention 108

On the occasion of the Data Protection Day, representatives of the Office of the Commissioner were invited to several national audio/visual media outlets to raise public awareness on the importance of protecting privacy and personal data.

Digital environment, series of awareness videos for teachers and pupils

The Information and Data Protection Commissioner’s Office introduced a series of awareness videos entitled “Guide for teachers of 9-year schools on the protection of personal data of pupils”. This 9-video series builds on the publication of the “Training framework for teachers of 9-year schools on the protection of pupils’ personal data”. This document was adopted by the 38th International Conference of Data Protection and Privacy Commissioners (ICDPPC), now known as the Global Privacy Assembly (GPA).

The Office of the Commissioner cooperates with the Roma Veritas Albania organization

The Office of the Commissioner signed a Memorandum of Understanding (MoU) in May 2021 with the organization “Roma Veritas Albania”, in support of its project “Legal education of Roma students, community mediators and health to facilitate access to justice for their community”. Earlier in March 2021, an online training was held with students and members of the Roma and Egyptian communities, to get acquainted with the constitutional rights of access to public information and the protection of privacy and personal data.

Complaints’ handling

During this period, **235** complaints were filed in accordance with the law on personal data protection.

Complaints mainly focused on:

- Violation of the rights of personal data subjects;
- Lack of personal data security (network data processing and online security);

- Disclosure of personal data in the media and online portals;
- Direct marketing in relation to unsolicited communications via telephone or e-mail.

Notification

In fulfillment of the legal obligation of controllers to notify about the processing of personal data, **35** controlling entities have notified. In addition, the statements of **18** controllers for change of the status of the previously notified processing were reviewed and administered.

The total number of processing notifications by controllers in the territory of the Republic of Albania has reached **5763**.

Administrative investigations

25 on-site inspections were carried out over this period, of which 19 with public controllers and 6 with private controllers. Inspections were initiated based on complaints (7), *ex officio* (18).

Main sectors under scrutiny were:

- Information and Communication Technology Sector;
- Telecommunication Sector.

The situation created by the pandemic conditioned and limited the on-site inspection activities compared to 2019. However, the Office of the Commissioner successfully addressed and implemented the recommendations set forth in the Resolution of the Parliament.

In more concrete terms, two working groups were set up to coordinate and execute tasks outlined in the recommendations in question. Subsequently, requests for information were addressed to 82 public institutions in the framework of identification and analysis of databases and online platforms under their administration. 68 institutions have responded.

After exhausting the preliminary verification process, administrative investigations were conducted with 9 public institutions, which were prioritised according to their area of responsibility and the relevance of their personal data processing operations, as well as based on the importance and frequency of public services that they provide. The inspections focused on the implementation of the legislation in force with respect to the security measures for the personal data, in order to guarantee their security with the establishment of the Information Security Management System (ISMS).

Inspections' findings

Some of the issues identified during the administrative investigations carried out with the controllers operating online platforms and information and communication technology are:

- Lack of a strategy or plan for the implementation of ISMS for personal data protection, which includes all components of a complete system for managing information security, in accordance with the applicable law;
- Deficiencies in addressing the obligations and legal guarantees related to the contractual relationships that public institutions (acting as controllers) establish with third parties (acting as processors) for the outsourcing of various services, where personal data processing constitute the essence thereof;
- Internal regulatory acts which provide only for general provisions on the handling of personal data and the protection of data subjects' confidentiality. Such acts, for the most part, are not sufficiently detailed with respect to the appropriate and applicable technical-organizational measures for guaranteeing the protection of personal and sensitive data, the lawfulness criteria of patients' data processing, the measures on ensuring traceability and control of the actions of persons/personnel holding access to such data, as well as the manner of their destruction when the processing purpose has been achieved;

- Lack of appropriate training of employees having access to personal data and the oversight of the processing activities and in terms of consolidating specific practices and legislation governing their activities. The requirements in terms of modernization of the infrastructure and the regulatory acts related to systems and databases remains to be addressed.

Recommendations- Administrative Sanctions - Hearing Sessions

In the ambit of the powers conferred to Commissioner by Law No. 9887/2008 "On the protection of personal data", as amended, the Commissioner has rendered:

- 6 recommendations for private controllers;
- 3 decisions with punitive fines which correspond to 9 administrative sanctions;
- 13 hearing sessions were carried out following the administrative investigation, and the relevant acts were subsequently rendered by the Office of the Commissioner.

With respect to international transfers, the Commissioner has issued 1 Decision to authorise international data transfer to countries that do not provide for an adequate level of personal data protection.

Legal framework - Alignment of national legislation with the GDPR

The legal framework in force on the protection of personal data is not in line with the GDPR and the Police Directive. Due to the importance of this reform and as a country aspiring EU integration, the Office of the Commissioner is the beneficiary of the twinning project "Support to the institution for the approximation of personal data protection legislation with the *acquis* of the European Union". This project aims at assisting the institution in the approximation of national legislation in force with the EU *acquis* in the field of personal data protection and to support the further development of the administrative capacities of Albanian institutions to implement this *acquis*.

The project kicked-off on 1 October 2020, and is being implemented by the Italian data protection authority, *Garante per Protezione dei Dati Personali*, supported by the Ludwig Boltzmann Institute for Human Rights (BIM), Austria and CSI - Piedmont, Italy. The project consists of three components:

Component 1: "Alignment of national legislation with the GDPR and the Police Directive", which aims to approximate the national legislation in force on personal data protection, with the EU *acquis* in this area.

Component 2: "Capacity building for enforcement of the new Data Protection legal framework", which aims at providing to the Office of the Commissioner with knowledge and organizational tools to address potential challenges related to the implementation of the new legal framework on the protection of personal data in Albania.

Component 3: "Awareness-raising with controllers and processors in order to ensure that they comply with the new Data Protection Law", which aims to provide all the latest knowledge and updates regarding the new Albanian law on personal data protection, through training of special focus groups from the public, private sector and civil society.

The staff of the Commissioner's Office in cooperation with the project experts have closely cooperated on preparing the draft law on the protection personal data. Work is currently underway for the implementation of the other two components of the project. The National Plan for European Integration envisages that the new draft law on personal data protection will be approved in the fourth quarter of 2021.

- Approval in principle of the amending protocol of CoE Convention 108

The Office of the Commissioner has worked on preparing the draft law "On the ratification of the amending protocol of Convention 108" "On the protection of individuals from automatic processing of personal data". With the Decision of the Council of Ministers No. 1001, dated 09.12.2020, it was approved in principle the amending protocol of Convention 108, whereas the procedures of signature and ratification are still ongoing. With the expected changes in the national legislation, Albanian citizens shall be guaranteed the highest standards in the field of personal data protection.

- **Draft Law on the Establishment of the Register of Unsolicited Commercial Communications**

The Commissioner's Office has prepared the draft law "On the establishment of the unsolicited marketing phone calls register", considering that this is the appropriate mechanism offering long term solution to the issue of unsolicited commercial communications. This draft law sets clear rules for the access, lawful administration and processing of personal data of citizens. For the consultation of this draft law, a working group was set with representatives of the Ministry of Infrastructure and Energy, the Electronic and Postal Communications Authority, as well as the Consumer Protection Agency within the Ministry of Finances and Economy. The draft law was submitted to the Parliament in the first quarter of 2021.

- **Other bylaws**

Pursuant to the obligations arising from the law on civil status, the Instruction No. 463, dated 10.12.2020 "On determining the institutions and bodies that receive personal data from the civil status service, as well as on the manner, type and amount of information they shall receive", was drafted in co-operation with the Ministry of Interiors. This act addresses developments in the use of new technologies in the provision of online state services.

In addition, pursuant to the obligations arising from the law on border control, the Instruction No. 464, dated 10.12.2020 "On the transmission of passenger data to the Passenger Information Unit" was drafted and approved in co-operation with the Ministry of Interiors. This act provides for unified standards relating to the supervision of the process of collection/processing, transmission and exchange of personal data of passengers. It further sanctions the manner of data transmission and the appropriate level of personal data protection by the Passenger Information Unit (PIU) within the State Police, in case of technical problems that hinders system's operability.

- **International relations**

The Information and Data Protection Commissioner was re-elected for an additional year as a full member of the Global Privacy Assembly's Executive Committee. The Commissioner was also reconfirmed as a member of the GPA Strategic Direction Subcommittee.

ARGENTINA / ARGENTINE

The following are the most important news on on the data protection field in Argentina:

(i) Appointment proceeding of the AAIP's Director

As you know, since December 31, 2020, Eduardo Bertoni is no longer the AAIP's Director.

On February 2021, the Executive Branch nominated the lawyer Gustavo Juan Fuertes as a candidate for Director of the AAIP (Resolution No. 100/2021).

Pursuant to the appointment proceeding set forth in Law No. 27.275, a public hearing was held on March 23, 2021, where Mr. Fuertes answered questions and addressed the objections to his nomination.

After the hearing was held, civil society organizations and legislators filed a series of objections in writing before the Head of Cabinet of Ministers, which interrupted the proceeding set forth in Law No. 27.275. Currently, the Executive Branch has to decide whether to confirm or discard the candidate's nomination.

You can find more information about the appointment proceeding in the following link:

<https://www.argentina.gob.ar/aaip/procedimiento-seleccion-director>

It is also important to note that, while the proceeding of appointment of the AAIP's Director is being resolved, Mr Eduardo Cimato is signing Resolutions and other official documents on behalf of the Agency, pursuant to Resolution AAIP No. 30/2018. The aforementioned Resolution establishes that the Director of the National Data Protection Directorate will be responsible for handling the Agency's matters during the temporary absence of the AAIP's Director.

<https://www.boletinoficial.gob.ar/detalleAviso/primera/183706/20180516>

(ii) New Comprehensive Data Protection Bill

On November 2020, national deputy Karina Banfi -along with co-authors Mario Raúl Negri, Gustavo Menna and Facundo Suarez Lastra- introduced to Congress a new Bill that proposes a comprehensive amendment to our current data protection law (Law No. 25.326). This is good news since this Bill relies partially on a Data Protection Draft Bill produced by the AAIP, that had been published on the AAIP's website in 2017.

The text of the [Bill introduced by deputy Karina Banfi](#).

AUSTRIA / AUTRICHE

The major developments since November 2020 are as follows:

- The annual report of the Austrian Data Protection Authority (Annual Report 2020) is available in German at <https://www.dsb.gv.at/download-links/dokumente.html>.
- The work of the Austrian Data Protection Authority has recently been dominated by the Covid pandemic, the associated questions that had to be answered immediately, and the efforts of all employees to ensure the authority's ability to function.
- The Austrian DPA was provided with more staff to handle the high number of complaints caused by the GDPR.

BOSNIA AND HERZEGOVINA / BOSNIE ET HERZÉGOVINE

BOSNA I HERCEGOVINA
Agencija za zaštitu ličnih/osobnih
podataka u Bosni i Hercegovini
Sarajevo



БОСНА И ХЕРЦЕГОВИНА
Агенција за заштиту личних података
у Босни и Херцеговини
Сарајево

No: 04-37-11-45-31/21

Date: 02 06 2021.

Secretariat T-PD

41st Plenary Session of the Convention Committee 108

dataprotection@coe.int

Subject: **The most significant activities in the field of personal data protection in Bosnia and Herzegovina for the period November 2020 - April 2021.**

Personal Data Protection Agency in Bosnia and Herzegovina was established by the Law on Protection of Personal Data („Official Gazette of Bosnia and Herzegovina“ 49/06) and began operations in June 2008. The current Law on Amendments to the Law on Personal Data Protection (Official Gazette of BiH No. 76/11) was adopted by the Parliamentary Assembly of Bosnia and Herzegovina in 2011.

Bosnia and Herzegovina has an obligation to align with the EU acquis under the Stabilization and Association Agreement (SAA), which it ratified in 2008 and entered into force on 1 June 2015. Regarding the process of harmonization of domestic legislation, the Agency has carried out all necessary activities to harmonize the Law on Protection of Personal Data with the latest data protection standards in force in the European Union. The Agency initially prepared a proposal for a new Law on Personal Data Protection, which was submitted to the Interdepartmental Working Group for drafting the Law, which continued to work on the Law. Interdepartmental working group (established according to the decision of the Council of Ministers of BiH from 2018) after the completed activities, submitted to the Ministry of Civil Affairs of BiH, as the legal proposer, the draft Law on Personal Data Protection for further procedure, which included public consultations and obtaining the necessary opinions of the competent institutions. At the session of the House of Representatives of the Parliamentary Assembly of BiH held on September 15, 2020, the Council of Ministers of BiH was ordered to submit the Draft Law on Personal Data Protection to the parliamentary procedure by the end of 2020, which has not been done so far.

The Rulebook on the internal organization and systematization of jobs in the Agency systematizes 45 jobs, and currently the Agency has 26 employees.

One of the legal obligations of the Agency is to monitor the situation in the field of personal data protection and to give suggestions, initiatives and opinions in this regard.

During the reporting period, the Agency prepared 13 opinions on various draft laws and bylaws, as follows:

The Ministry of Justice of BiH was given opinions on the Draft Law on Protection of the Right to Trial within a Reasonable Time, on the Draft Law on Amendments to the Law on the High Judicial and Prosecutorial Council of Bosnia and Herzegovina, on the Draft Law on Amendments to the Law on Execution of Criminal sanctions, detention and other measures and the Draft Law on Prevention of Conflicts of Interest in the Institutions of Bosnia and Herzegovina; The Ministry of Finance of BiH was given an Opinion on the Draft Law on the Budget of the Institutions of Bosnia and Herzegovina and International Obligations of Bosnia and Herzegovina for 2021; The House of Representatives of the Parliamentary Assembly of BiH was given opinions on the Proposal of the Law on Amendments to the Law on Salaries and Remunerations in the Institutions of Bosnia and Herzegovina, on the Proposal of the Law on Amendments to the Law on Labor in Institutions of Bosnia and Herzegovina, on the Proposal of the Law on Prevention of Conflict of Interest in the Institutions of the Government of Bosnia and Herzegovina and on the Proposal of the Law on Amendments to the Law on Aliens; The General Secretariat of the Council of Ministers of BiH was given an Opinion on the compliance of the provisions of the Decision on Framework Criteria for Awarding Cash Rewards to Employees in the Institutions of Bosnia and Herzegovina with the Law on Personal Data Protection; The Civil Service Agency of Bosnia and Herzegovina was given an opinion on the Proposal of the Decision on the manner and procedure

Sarajevo / Сарајево, Dubrovačka broj 6 / Дубровачка број 6
tel/fax +387 33 726-250, fax/fax +387 33 726-251

of submitting the electronic application of candidates in the procedure of employment of civil servants; The Ministry of Civil Affairs of Bosnia and Herzegovina was given an opinion on Article 17 of the Draft Agreement between the Council of Ministers of Bosnia and Herzegovina and the Government of the Republic of Poland on cooperation in culture, education, science and youth between the Council of Ministers of Bosnia and Herzegovina and the Government of Poland.

The scope of providing expert opinions and responses to the requests of controllers and holders of personal data has decreased in this period of the Covid-19 pandemic. In the reporting 6 months, 64 expert opinions and 84 responses were issued instead of expert opinions to the requests of the public and private sector.

Through the inspection, the Agency supervises the fulfillment of obligations prescribed by the Law on Personal Data Protection. In performing its regular supervisory activities, in the reporting period, due to restrictions caused by the Covid-19 pandemic, the Agency performed only 9 regular and 3 extraordinary inspections, and 8 decisions were made on regular inspections and 5 decisions on the controller's appeal. Also, 36 decisions and 4 conclusions were issued ex officio, and 110 acts related to cases ex officio.

In the reporting period, 5 judgments of the Court of Bosnia and Herzegovina were rendered in favor of the Agency, 10 responses to the lawsuit were submitted, and 3 requests for review of the court decision were made.

The number of complaints filed by citizens during the pandemic indicates an increase in awareness of the importance of personal data protection. In the reporting period, 54 decisions and 13 conclusions on complaints were made, mostly against public bodies, but also other controllers, economic entities and natural persons, and 147 activities were performed in the procedure of resolving complaints.

The Agency started issuing misdemeanor warrants in 2011, and 7 misdemeanor warrants were issued in the reporting period.

Regarding the activities of the Main Registry, 46 new controllers were registered and 201 new databases were entered. By the end of April 2021, a total of 943 controllers and 4,907 collections of personal data were entered in the Main Register.

In the reporting period, Agency officials participated in 5 online conferences, 12 meetings, 1 presentation and 5 trainings.

The Agency regularly informs the media about its competencies and activities, promotes the work of the Agency and informs the public regarding the processing and protection of personal data. The Agency usually responded to all media inquiries and reported on time through all available media, publishing opinions and solutions, and other useful information on the Agency's official website, as well as through the Help Desk.

In connection with the above, a Press conference was held on the occasion of the European Data Protection Day in Bosnia and Herzegovina on January 28, 2021, 3 press releases were given, 12 written answers, 2 statements and 3 guest appearances were given to various inquiries of print and electronic media. 162 inquiries from citizens were answered through the Agency's Help Desk.

The Agency's website is regularly updated with the necessary content. In the reporting period, 109 publications of various numbers (ie 272 pages) were posted on the Agency's website www.azlp.ba, and 15 articles related to the Agency's activities and personal data protection were published in the media and on the Internet. In the reporting period, 9692 visits to the Agency's website were recorded.

Kind regards,

Submitted:

- To the title
- a/a



Director
dr. Dragoljub Reljić

Sarajevo / Capajevo, Dubrovačka broj 6 / Dvobrovačka broj 6
tel/fax +387 33 726 250, fax/fax +387 33 726 251

BULGARIA / BULGARIE

Commission for personal data protection

Major Developments in the Data Protection Field

October 2020 – May 2021

Introduction

The main objective of the Commission for Personal Data Protection (Commission, CPDP) in its capacity as a national supervisory authority is the implementation of an effective supervisory mechanism in the field of personal data protection.

Previous information

Shortly after the implementation of the new regulation on personal data protection between 22 and 26 October 2018, the Commission for Personal Data Protection and the European Data Protection Supervisor hosted the most important International Conference of Data Protection and Privacy Commissioners ((ICDPPC) now Global Privacy Assembly (GPA)) in the field of personal data protection. The 40th Conference took place under the title „Debating Ethics: Dignity and Respect in Data Driven Life”. For the first time, the conference is co-organized by a European institution and a national data protection authority.

Legal Framework

On the 26th of February, 2019, the Bill on Amendment and Supplement of the Data Protection Act adopted by the 44th National Assembly on the 24th of January, 2019, re-adopted on the 20th of February, 2019 by the veto of the President of the Republic of Bulgaria, has been promulgated officially in the 17th issue of the State Gazette.

On the 11th of September 2019 the National Assembly of the Republic of Bulgaria ratified by law the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention SETS No. 223)

Activities during a period of pandemic

The activities of the Commission for Personal Data Protection of the Republic of Bulgaria (Commission, CPDP) were influenced by the Coronavirus disease (COVID-19) pandemic like all other spheres of public life. Yet, the CPDP succeeded in organising its work for ensuring continuity of the administrative services and exhaustively participating in events at the international level via remote access.

2020 was a very active year for data protection and the right to privacy, and the Bulgarian data protection authority experienced an increase in the number of complaints received and the actions taken throughout the year. The most violations were made by data controllers processing personal data via established video surveillance systems as well as in the field of telecommunication services, media, banks and marketing companies.

The COVID application was launched in Republic of Bulgaria in May 2020. The app is called Virusafe and the application aims to help in the fight against COVID-19, allowing each user to regularly enter their symptoms, as well as to monitor the development of the pandemic with a map that shows where and how many infected users there are by region in Bulgaria at the moment.

In 2020, the Commission for Personal Data Protection organizes a competition for a student essay on "Emerging technologies and personal data protection - legislation and practical application." As five candidates were admitted to the finals and the winning essay is entitled "May 2020, humanity is experiencing catharsis, the world is facing the biggest challenge so far, and technology is about to take over our familiar world and replace it with a completely a new universe of rules and boundaries". The winner received a diploma, a cash prize, a smartphone and a paid one-month internship at the Commission for Personal Data Protection.

On 28 January 2021, the Commission for Personal Data Protection marked the Data Protection Day once again with a number of events, as well as the launching of initiatives aimed at raising the awareness of citizens and establishing an inner value system with regard to the better understanding of personal data processing policies.

The following activities were implemented:

1. Reception room for personal data controllers/processors and individuals – the citizens (individuals, data controllers, other organisations concerned) with the opportunity to ask questions on data protection issues.
2. Special annual prize was awarded by the CPDP for the fifth time to the media for raising awareness in the data protection field and about the CPDP's activities.
3. E-Congratulations Letter to all designated data protection officers in Bulgaria accompanied by additional information will be circulated.
4. Direct links were posted on CPDP website to the EDPB initiatives, including the prepared video by the Board on the occasion of 28 January celebration, which the Secretary General of the CPDP took part in.
5. Official presentation of the digitally developed self-assessment tool for SMEs – SMEDATA project deliverable.

International Cooperation

One of the priorities of the Commission for Personal Data Protection of the Republic of Bulgaria is an effective cooperation with international organisations and its counterparts in foreign states.

For more than 10 years the Commission for Personal Data Protection has been an accredited member of the Global Privacy Assembly and continues to take an active part in it. A representative of the Commission took part in the 42nd edition of the Forum from 13 to 15 October 2020.

The Commission actively participates in the current working program of the European Commission, actively participating in the development and negotiation of the full package of documents related to the protection and free movement of personal and non-personal data.

At the establishment of the European Data Protection Board, the Chairman of the Bulgarian DPA, Mr. Ventsislav Karadjov was elected as the Vice-Chairman of the European Data Protection Board (EDPB).

The CPDP participates in all current processes for the implementation of the tasks of the EDPB. These include preparation and participation in EDPB plenary sessions and working groups. The realized full technical compliance with the Committee's communication systems allowed participation in the meetings of the separate working groups, remotely.

During the reporting period, representatives of the CPDP continued their participation in the work of the joint supervisory authorities and coordination groups for the supervision of large-scale EU information systems: the Europol Cooperation Council, the Customs Information System Supervision Coordination Group, the Schengen Information System II Supervision Coordination Group, The Visa Information System Supervision Coordination Group, Eurodac Supervision Coordination Group and the Internal Market Information System.

Activities of the CPDP related to the promotion of the right to protection of personal data

In pursuance of the Commission's priorities, it developed and approved key documents as follows:

1. Instruction for practical implementation of the supervisory activity of the CPDP (the instruction is fully in accordance with the guidelines adopted by the European Data Protection Board in January 2021: Guidelines for the application of Article 62 of Regulation 2016/679 (internal document intended only for data protection authorities to regulate the implementation of joint operations between those supervisory authorities).
2. Methodology for risk assessment in cases of personal data breaches (the methodology is an appendix to the Instruction for practical implementation of the supervisory activity of the CPDP. The document is a tool for risk assessment of the rights and freedoms of persons whose data are breached;
3. Questionnaire for carrying out inspections as part of the CPDP surveillance operations (the questionnaire is applicable to all types of inspections carried out by the Commission and its administration).

CAPE VERDE / CAP VERT

Commission Nationale de Protection des Données

Activités réalisées de novembre 2020 à juin 2021

Dans le cadre de l'initiative législative de modification du régime juridique de protection des données personnelles des personnes physiques et de la loi fixant la composition, la compétence, l'organisation et le fonctionnement de la Commission nationale de protection des données (CNPDP), le président et d'autres membres ont été reçus lors d'une audition du Président du Parlement et des Chefs des groupes parlementaires des partis politiques afin d'obtenir le soutien de sa programmation et, par conséquent, son approbation, qui s'est tenue à l'unanimité le 11 février 2021.

La CNPDP a reçu à son siège, pour une réunion de travail, un haut responsable d'INTERPOL dans le but de fournir des informations sur l'engagement de la CNPDP dans le partage des données personnelles entre cette organisation internationale, la Police Judiciaire Cap-Verdienne et les autorités police de la CEDEAO.

Appelé par la CNPDP, le responsable national du Programme de lutte contre le VIH-SIDA a été entendu sur le détail des données personnelles des personnes atteintes du VIH-SIDA.

La CNPDP a reçu, en visite de travail, le Médiateur. Les deux institutions ont conclu à la nécessité de mener des actions communes, car il existe des points de convergence dans la défense des droits des citoyens. En conséquence, il y a eu une formation des techniciens du Bureau du Médiateur sur la protection des données personnelles.

Il y a eu une réunion de travail avec la Plateforme des organisations de la société civile dans le but de sensibiliser les membres de cette institution au respect des dispositions légales et réglementaires relatives au traitement des données personnelles, notamment des personnes les plus vulnérables.

Le 8 février 2021, la CNPDP a organisé un webinaire avec l'Association des Dentistes sur le thème du Traitement des données personnelles sensibles des patients dans le cadre de la gestion des dossiers cliniques.

Les 13 et 14 avril 2021, la CNPDP a organisé un Webinaire visant à socialiser les principales évolutions du régime juridique général de protection des données personnelles des personnes, avec la présence de la Banque centrale, des banques commerciales, des opérateurs de télécommunications, des entreprises technologiques, Institut National de la Statistique, Institut National de la Santé Publique, Police Nationale, Police Judiciaire, Agence Multisectorielle de Régulation de l'Economie et Médiateur.

La Commission nationale de protection des données a également organisé des conférences sur le traitement des données de santé dans deux hôpitaux centraux et dans une université publique.

La CNPDP a accordé une interview à Paradigm Initiative (Nigeria) dans le cadre de la cartographie des autorités de protection des données sur le continent africain.

Concernant la diffusion une vidéo a été diffusée sur le traitement des données des consommateurs pendant le temps d'antenne de l'association nationale de protection des droits des consommateurs et des dépliants ont été produits, notamment sur les achats en ligne et le traitement des données de santé.

La CNPDP a accordé deux interviews à des chaînes de télévision nationales sur les achats en ligne et le risque pour la vie privée et la protection des données personnelles sur Internet.

Parmi les avis émis, celui concernant le transfert de données personnelles à l'autorité de réglementation de la santé par les cliniques dentaires se démarque.

CROATIA / CROATIE

The major developments in the data protection field in our country and organization since November 2020

During the mentioned period, Croatian Personal Data Protection Agency handled hundreds of cases and many of them were related to the area of international cooperation meaning the Agency's cooperation with the bodies responsible for supervising the processing of personal data of the Member States of the European Union. The Agency also records continuous cooperation with EU institutions and international organizations and other countries - directly or through domestic competent institutions, for example on the basis of cooperation with the Ministry of Foreign and European Affairs and through the participation of both NGOs and AZOP within expert working groups related to legal proposals and within the framework of the Open Government Partnership, which is led by the Ministry of Foreign and European Affairs with the assistance of the Office of the Government of the Republic of Croatia for Cooperation with NGOs.

Additionally, in 2021, the primary adjustment of the Agency in the work and implementation of supervisory activities in the COVID-19 environment was support from the aspect of personal data protection to competent state institutions on legislative and technical-operational issues (e.g. amendments to relevant regulations and introduction of information systems / solutions and application).

Regarding supervisory activities, according to the Article 36 of the Act on the Implementation of the General Data Protection Regulation (OG 42/18) authorised employees of the Agency carried out:

-102 direct supervisions (16 announced and 85 unannounced supervisions)

-11 indirect supervisions

Following the notification on the designation of data protection officers the total number of notifications that Agency received as a supervisory authority in the period from 01.11.2020. since 01.06.2021. is 1025.

Regarding the media, in the above-mentioned period Agency received and acted upon 40 press inquiries.

Pursuant to Article 14 of the Act on the Implementation of the General Data Protection Regulation (OG 42/18), the Agency provided over 70 expert opinions on drafts of proposals of laws and proposals of other regulations governing issues related to personal data processing regarding the area of personal data protection.

On the European Data Protection Day which we celebrate on January 28th, Croatian Personal Data Protection Agency organized the international online conference ***Digital transformation and data protection in a pandemic world.***

The conference focused on micro, small and medium-sized entrepreneurs who are the most affected group by the global pandemic of the economic system in the Republic of Croatia, as well as in the entire European Union. During the global pandemic, data protection and digital transformation have become key factors for their survival on the market. Small and medium-sized enterprises must address more proactively challenges and develop a comprehensive strategy for digital business transformation to respond to the current crisis. The key message we wanted to send to entrepreneurs and to the

general public is that investment in compliance with the General Data Protection Regulation, digital transformation, and information security is a worthwhile investment and not an administrative burden. Furthermore, it is also an opportunity to increase operational efficiency and to successfully exploit the business opportunities that the COVID-19 crisis has brought. The Croatian DPA and other public institutions are here to help SMEs and to offer support in their efforts, as well as to protect the fundamental rights of the citizens.

In order to provide SMEs with the necessary support in complying with the GDPR, Croatian Personal Data Protection Agency has been coordinating the implementation of the EU project ARC-Awareness Raising Campaign for SMEs since March 2020. (data protection awareness campaigns for micro, small and medium-sized enterprises), co-financed by the European Union's Rights, Equality and Citizenship Programme. This significant project is being implemented by AZOP in cooperation with the Data Protection Commission Ireland and the University Vrije Bruxelles. The ARC aims to support SMEs in aligning with the GDPR through the implementation of various project activities, such as holding advisory activities and developing educational materials tailored to the specific needs of micro, small and medium-sized enterprises. Project activities will run until March 2022. The Croatian Chamber of Economy provides support to AZOP in the organization and implementation of all activities.

Project activities aim to support medium and small entrepreneurs in compliance with the GDPR requirements, but also to raise the level of awareness of personal data protection among the general public.

On 25th May 2021., the third anniversary of the full implementation of the General Data Protection Regulation, the Croatian Personal Data Protection Agency held an international conference **"GDPR 3 years on: The experiences and challenges of the European SMEs"**, which was organized together with partners in the ARC project. The conference was organized to present the project results of the ARC project and was intended primarily for entrepreneurs and their experiences in complying with the GDPR during the 3 years since the GDPR was fully implemented, but also brought together many foreign and domestic experts in the field of data protection, information security and IT sector. The key message of the conference is that the GDPR is not a burden or an obstacle, but an opportunity for entrepreneurs to improve their business and gain an advantage in the market over competitors who do not respect the fundamental human right to data protection. All conference participants highlighted the importance of educating entrepreneurs and the principle of "better to prevent than to cure". It is very important that entrepreneurs are well informed about their obligations under the legislative framework on data protection, harmonize their business and thus avoid situations in which they may find themselves in the role of violators of the General Data Protection Regulation and therefore incur high financial sanctions.

In a tender conducted by the European Commission on March 10, 2021, the Croatian Personal Data Protection Agency was selected to implement a Twinning project entitled **"Supporting the implementation of a modernized legislative framework for personal data protection"** in Northern Macedonia. The aim of the project is to improve the area of personal data protection and the national system of personal data protection in Northern Macedonia in accordance with the European acquis. This significant international success is due to AZOP's team of experts led by the Director of the Croatian Personal Data Protection Agency. The Croatian Personal Data Protection Agency is extremely honored and pleased to be able to contribute to the reputation of the Republic of Croatia in the European Union in this way.

Further work of the Agency will consist of effective action to fulfill all rights and obligations in the field of personal data protection, with a strong focus on improving and increasing the responsibility of all participants in the process of personal data processing with emphasis on compliance with legal

regulations. Priority areas will be developed in accordance with the upcoming situation and possible problems, but certainly by elaborating the issues related to the COVID-19 situation and the processing of personal data related to it.

CYPRUS / CHYPRE

The Cyprus Commissioner for Personal Data Protection since December 22nd 2020, is also acting as Information Commissioner after the entry into force of the Right of Access to Public Sector Information Law 2017 (184(I)/2017). The Law establishes the rights of citizens to request and receive, under certain conditions, information held by public bodies.

The Commissioner has issued guidelines in January 2021, on the use and processing of personal data in the context of the political communication during the Parliamentary elections' campaign period (Elections of May 30, 2021).

The Commissioner throughout the Pandemic period has been actively engaged and provided guidelines and opinions in the context of prior consultation with the competent Ministries for the purpose of dealing with specific personal data protection issues in certain domains.

The Commissioner is also trying to keep the citizens' / data subjects well aware of their rights and data processing procedures during the pandemic period by means of written communications /press releases, interviews and Frequently Asked Questions uploaded on the website.

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

The necessity of adapting the Czech law to the fight against the spread of SARS-CoV-2 was handled predominantly, mainly through the Act on extraordinary measures during the COVID-19 pandemic as well as via the amendment to the Act No. 258/2000 Coll., on protection of public health. On the one side, it can be appreciated that these legal provisions offered proper legal grounds for the processing of personal data (e-Facemask application – eRouška in Czech, establishment of a call centrum). On the other side, we cannot look away from the absence of sufficient safeguards in terms of the protection of personal data and privacy.

Further activities worth mentioning involve the co-work on the act on digitalization of the health sector (eHealth), on the issue of disclosure of property and conflict of interest declarations by municipal public functionaries and last but not least on the implementation of the duty for executors to record phone calls. Our authority promoted introduction of appropriate data protection safeguards in all mentioned instances.

Essential changes are expected to be introduced by the currently prepared act on identity cards. The discussions surround namely the re-assessment of the scope of information contained in the identity cards including the implementation of biometric data. This act should also reflect the need for further development of the eGovernment project. In future, the identity cards should not bear the birth certificate number any more, whilst our authority supports the successive elimination of this data element as a general identifier. The birth certificate number (or simply the birth number) shall in the private sector be replaced by an identifier not enabling to learn the date of birth and the sex of the given individual.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) / LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

Update on the European Data Protection Supervisor's activities (November 2020- May 2021)

1. Supervising European institutions, bodies and agencies

Using the tools at our disposal, the European Data Protection Supervisor continues to supervise and monitor European institutions', bodies' and agencies' (EUIs) compliance with the applicable data protection law, [Regulation \(EU\) 2018/1725](#).

Data protection amid a global health crisis

Like many other organisations, the EDPS has continued to adapt its work due to the continuing COVID-19 pandemic. To support EUIs in protecting individuals' data during this time, the EDPS produced a series of Guidelines. For example, in February 2021, the EDPS issued [Orientations](#) on the use of manual contact tracing by EUIs in the context of the COVID-19 crisis as this involves the collecting, sharing and storing of highly sensitive personal information, such as medical and health data. As such, the EDPS recommends that medical professionals, such as an EUI's medical officer, should be in charge of processing health data and to respect the privacy of the individuals involved.

As well as other initiatives, the EDPS organised a webinar in January 2021 entitled [Data for the public good: Building a healthier digital future](#). The aim of the event was to assess, in broad terms, the impact of the measures taken in response to the COVID-19 pandemic and identify ways in which data can be used to be better prepared for the next one. Experts from various fields addressed three main themes, namely public health; digital transformation; and the impact on fundamental rights, such as freedom of movement, data protection and non-discrimination.

International transfers of personal data

The topic of international transfers of personal data remained high on the EDPS' agenda, in particular on how EUIs can comply with the ["Schrems II" Judgement](#).

In December 2020, the EDPS met with the EUIs' network of data protection officers (DPOs). This [online meeting](#) focused on issues related to international transfers in light of the EDPS' recently published [strategy for EU institutions to comply with the "Schrems II" Judgement](#). Questions predominantly focused on technical details, such as the practical consequences for existing and new contracts, how to conduct Transfer Impact Assessments (TIAs), or the margin of manoeuvre with regard to the use of derogations or supplementary measures.

As part of our *strategy for EU institutions to comply with the "Schrems II" Judgement* issued in October 2020, we [launched two investigations](#) on 27 May 2021 to ensure that ongoing and future international transfers are carried out according to EU data protection law. The first investigation concerns the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EUIs. The second investigation concerns the use of Microsoft Office 365 by the European Commission. The EDPS decided to launch these investigations following the outcome of the reporting exercise on their international transfers which it ordered EU institutions and bodies to carry out. The EDPS' analysis shows that because of diverse processing operations, when using tools and services offered by large service providers, individuals' personal data is transferred outside the EU and to the United States (US) in

particular. Our work in this area is an example of a continuous cooperation between the EDPS and the EUIs to ensure a high level of protection of these fundamental rights.

EDPS Audits

We carry out audits in the EUIs as part of our supervisory work, allowing us to verify how data protection is applied in practice. Recently, on 28 April 2021, we [published](#) the outcome of our remote audit on how EUIs inform individuals about the way their personal data is processed when signing up to newsletters or other subscriptions. We found that most EUIs comply with the information on transparency requirements set out in Regulation (EU) 2018/1725. Due to the COVID-19 pandemic, we have carried out remote audits; a format which has allowed us to continue our supervisory work by reaching out to a high number of EUIs, their DPOs, and EUI staff processing individuals' personal data in their day to day work.

Training sessions for EUIs

The EDPS pursued its online training sessions on themes that we identify as areas in which further clarity or assistance is needed to ensure EUIs' compliance with Regulation (EU) 2018/1725.

With the increase of remote working due to the COVID-19 pandemic, regular training sessions for EUIs and their staff were held on [the use of ICT tools, remote working tools and the use of social media](#). The purpose of such training sessions is to ensure that EUIs choose carefully these tools to protect individuals and their personal data.

Other training sessions were organised on the [outsourcing of the processing of personal data and procuring products and services](#), for example. These sessions, among other topics, focused on the application of data protection requirements during the different stages of the procurement and outsourcing process: from the call for tender to signing the contract with an external organisation. The EDPS advises EUIs to periodically re-evaluate their processing operations, their tools, and their data protection safeguards and measures - this also includes data protection safeguards and measures in their contracts with external organisations - and readjusting these if necessary.

2. Our Policy and Consultation work

The EDPS continues to act as an advisor to the EU legislator on data protection issues. Our aim is to ensure that data protection requirements are integrated into all new legislation, policy initiatives and international agreements. As such, we provide guidance to the European Commission, the European Parliament and the Council in the form of [Opinions](#) and both [Formal](#) and Informal Comments.

Of particular note, we issued an Opinion on the proposed [New Pact on Migration and Asylum](#) in November 2020. Data protection is one of the last lines of defence for vulnerable individuals, such as migrants and asylum seekers approaching the EU external borders. The EDPS therefore advises, among other considerations, that an in-depth assessment of the impact that this proposal may have on data protection and fundamental rights is carried out.

Another notable Opinion issued in November 2020 is our [Preliminary Opinion](#) on the [European Health Data Space](#) (EHDS), which is part of the European Commission's European strategy for data. In its Preliminary Opinion, the EDPS highlights that data protection laws - such as the GDPR - and appropriate safeguards should be embedded in the development of the EHDS due to the sensitive nature of the information being processed.

More recently, in February 2021, the EDPS [published](#) an Opinion on the two proposed agreements between the EU and the United Kingdom: the Trade and Cooperation Agreement (TCA) and an agreement on the security procedures for exchanging and protecting classified information.

The EDPS also issued a number of Formal Comments on wide-ranging topics, the latest were on a package of three legislative proposals for a [European Health Union](#). These proposals aim to improve the protection, prevention, preparedness and response to human health hazards at EU level.

3. Monitoring Technologies

The EDPS monitors the impact of new technologies on data protection and on individuals' personal data.

Notably, on 11 March 2021 the EDPS published an Opinion on the [Proposal for the NIS 2.0 Directive](#), which aims to replace the existing Directive on security of network and information systems (NIS). The Proposal is part of the [EU's Cybersecurity Strategy](#) to ensure a global and open internet with strong safeguards to mitigate the risks for individuals' fundamental rights, including the right to data protection. The EDPS' Opinion includes remarks and recommendations on both the Strategy and the proposed Directive. Among these, the EDPS stresses that compliance of all practical measures, such as the use of cybersecurity systems to prevent, detect and respond to cybersecurity threats, with EU data protection law is imperative. The EDPS also emphasises that the use encryption, in particular end-to-end encryption is crucial.

Through its various publications, like the [TechDispatch reports](#), the EDPS explains emerging developments in technology and assesses their impact on privacy and data protection. Since November 2020, the EDPS has released two TechDispatch reports, one on [Personal Information Management Systems](#) and one [Facial Emotion Recognition](#), available on the EDPS website.

Recently, the EDPS also cooperated with the Spanish data protection authority, Agencia Española de Protección de Datos (AEPD), on a Joint Paper entitled [10 misunderstandings related to anonymisation](#) to bring clarity on what data anonymisation means and contribute to clearing up any misconceptions surrounding this topic.

To help both the EDPS and the European Data Protection Board's (EDPB) staff, the EDPS has started to organise regular trainings, for example on [cybersecurity](#) to ensure that they can protect themselves, their institution, as well as other individuals, against such threats, especially in times of teleworking.

As well as raising awareness of the impact of technologies on data protection and individuals' privacy, the EDPS has continued to improve its [Website Evidence Collector](#) (WEC). The WEC is an open source software tool with the aim to help data protection authorities, data controllers, data protection practitioners and web developers to carry out their own website inspections and to better understand which information is stored during a website visit. In January 2021, the EDPS made its version 1.0 [available](#) to the public. With this update, the tool received a number of new configuration options to improve its use.

4. The EDPS as a member of the EDPB

The EDPS provides an independent secretariat to the European Data Protection Board ([EDPB](#)), which is an independent European body contributing to the consistent application of data protection rules throughout the European Union (EU Member States). The EDPS is also a member of the EDPB and cooperates with the other data protection authorities of the EU. [A Memorandum of Understanding](#) determines the terms of cooperation between the EDPB and the EDPS.

Through this cooperation, the EDPS and EDPB have issued several Joint-Opinions towards the end of 2020 and in the first half of 2021, such as the [Joint-Opinion](#) on the Digital Green Certificate proposals and the [Joint-Opinion](#) on the Data Governance Act.

In addition, the EDPS and the EDPB have worked together on the topic of transfers of personal data to non-EU countries. For example, the EDPS actively contributed to the drafting of [Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#), and the [Recommendations on the European Essential Guarantees for surveillance measures](#) published on 10 November 2020. These documents were adopted after the '[Schrems II](#)' ruling to ensure that ongoing and future international data transfers are carried out according to EU data protection law. [Two Joint Opinions](#) were also issued in January 2021 on two sets of contractual clauses (SCCs), one Joint-Opinion on SCCs for contracts controllers and processors, and one Joint-Opinion on the SCCs for the transfer of personal data to third countries.

ESTONIA / ESTONIE

About major developments in data protection field from November 2020-2021

1. Estonian Data Protection Inspectorate - activities in numbers

The main statistical figures summarizing the year 2020

- Data breach notifications (based on the art 33 of the GDPR9): 138
- Received complaints and challenges: 701
- Information requests and explanations: 1759
- Help-line calls: 1222
- Opinions on draft legislation: 29
- Fines imposed: 12

2. Relevant trends – awareness raising in a “new way”

Tests for data subjects

The Inspectorate has always considered it important to contribute to awareness-raising training, counselling, and the creation of guides. In order to explain the principles of data protection and to prepare for finding the right answers for oneself, the Inspectorate conducted 2 online tests: '[Andmekaitse ja raketiteadus](#)' (Data protection and rocket science?) and '[Digivegan](#)' (Digital vegan).

The aim of the 'Digivegan' test was to give the test-takers the opportunity to find out whether they are environmentally conscious in terms of the digital life in their everyday computer activities. Whether a person is careful with their personal data, i.e. does not share them with just anyone, is an important part of data protection.

The test 'Andmekaitse ja raketiteadus?' allowed people to test their basic knowledge of data protection principles. Once a person has made the principles clear, they will be able to find the right answers in any situation with less effort. After all, no service can function without the use of personal data, and there are practically no areas that are not covered by data protection.

IT-based tool for creating a 'Video surveillance' sign

The Inspectorate, in cooperation with the Centre of Registers and Information Systems, also created a video surveillance sign generator, which helps the video surveillance organiser to obtain a proper notification sign file either for printing or sending to a printing house

By creating a video surveillance sign with the generator, the person is also explained why it is important to add the required information to the sign and what it should look like exactly.

The easiest solution is to use the video surveillance sign generator on the website of the Data Protection Inspectorate – videovalvesilt.aki.ee.

Video seminars

In previous years, the Inspectorate has organised trainings, seminars, and conferences on the topics of the Personal Data Protection Act and the Public Information Act. However at the end of the 2020, the Data

Protection Inspectorate started [a series of video seminars](#). The added value of video seminars is that they can be watched at any time and as many times as needed.

The first web-streamed video seminar was aimed at employees of educational institutions and explained data protection issues in distance learning and document management. The participants of the video seminar could ask questions both before and during the seminar.

In 2021, video seminars were continued for the apartment house associations, but also about using the video-surveillance in employment relations and making analytics based on video-surveillance.

FINLAND / FINLANDE

Legislative developments

Finland ratified the Protocol amending Convention 108 on 10 December 2020. The related amendments to the Data Protection Act (1050/2018) and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018) entered into force on the same day. The amendments concern cooperation between the Data Protection Ombudsman and the data protection authorities of countries that are not member states of the EU. In addition, in the Act 1054/2018, most derogations concerning the processing of personal data in the context of national security were repealed.

The Ministry of Justice has initiated an overall review of the Act on the Openness of Government Activities, lasting until the end of June 2023. The Act includes, among others, generally applicable provisions on the disclosure of data from personal data files maintained by public authorities. In addition, a major project has been initiated by the Ministry of Finance on redesigning the system of personal identity codes. The purpose of the project is to ensure there are sufficient personal identity codes available, allow gender-neutral personal identity codes, enable foreign nationals to conduct their affairs more conveniently by broadening the eligibility for personal identity codes, and produce guidance on using personal identity codes and other related core personal data in Finland. One of the aims is to reduce the use of personal identity codes in situations where identification is required. The project term is from 1 December 2020 to 31 December 2022.

The work on the alignment of the provisions on the processing of personal data with the data protection framework of the EU is still ongoing for part of the special legislation. The legislative work in the past year has been affected by measures taken to combat Covid-19, which has also to some extent slowed down the review of legislation. The measures related to Covid-19 have also involved important questions of data protection.

Data Protection Ombudsman

At the Office of the Data Protection Ombudsman, the year 2021 started with a Data Protection Day online event on 28 January. The main themes for this year's event included personal data breaches and international data transfers.

In February, the Office of the Data Protection Ombudsman published the accreditation criteria for code of conduct monitoring bodies.

The Office of the Data Protection Ombudsman and the Finnish Information Society Development Centre (TIEKE) were granted EU project funding in 2020 in order to produce an easy-to-use tool for small and medium-sized enterprises. The GDPR2DSM project was launched in the spring with a survey aiming to identify the data protection needs of SMEs and the challenges they have encountered in the application of the GDPR.

In addition, the Office of the Data Protection Ombudsman commissioned a survey to chart the views of stakeholders and citizens on its operations and reputation. The results show that the Office is valued for its expertise and reliability but room for improvement is seen in customer orientation.

FRANCE

I. Projet de loi autorisant la ratification du Protocole n°223

Le Gouvernement de la République française a signé à Strasbourg le 10 octobre 2018, le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Protocole n°223).

A l'issue du processus de consultations interministérielles et après avis du Conseil d'État, le projet de loi autorisant la ratification du Protocole 223 a été présenté par le ministre délégué auprès du ministre de l'Europe et des Affaires étrangères, chargé du Commerce extérieur et de l'Attractivité, lors du Conseil des Ministres du 5 mai 2021.

Le projet de loi déposé au Parlement, sera prochainement examiné par la Commission des affaires étrangères, de la défense et des forces armées du Sénat.

II. La CNIL – Développements et actualités récents

La CNIL a connu des temps fort avec la crise sanitaire et de nouvelles règles en matière de cookies, de cybersécurité et de souveraineté numérique. Les derniers mois ont par ailleurs été marqués par un nombre de plaintes toujours plus élevé et une augmentation considérable des violations de données, trois ans après l'entrée en application du RGPD.

LES TEMPS FORTS DE 2020

1. COVID-19 : la protection des libertés et des données personnelles au cœur des débats publics

Dans le contexte de la crise sanitaire, l'utilisation des technologies de communication à distance et de dispositifs de surveillance pour essayer de ralentir l'épidémie ou pour s'adapter aux mesures de distanciation physique n'a cessé d'augmenter. Face à la multitude d'initiatives, la CNIL a su mobiliser ses deux piliers, l'accompagnement et la chaîne répressive, tout en restant à l'écoute de ses publics.

Tout au long de l'année, la CNIL a ainsi conseillé activement les pouvoirs publics afin de contribuer à garantir que la mise en œuvre des systèmes d'information sanitaires (StopCovid-TousAntiCovid, SI-DEP, Contact Covid, Vaccin Covid) soit respectueuse des droits des personnes concernées. La participation de la CNIL à la coopération européenne a également permis d'apporter des positions communes importantes, notamment sur les applications de suivi de contact ou le traitement de données de santé à des fins de recherche scientifique dans la lutte contre le virus.

Afin de répondre à un grand nombre d'interrogations des particuliers et des professionnels, la CNIL a su proposer sur son site des contenus inédits tels que ceux publiés sur la continuité pédagogique, le télétravail, la distribution de masques par les collectivités ou encore TousAntiCovid.

Par ailleurs, la CNIL a priorisé le traitement des plaintes liées à la COVID-19 ainsi que les contrôles des dispositifs mis en œuvre, et a mené des contrôles sur des sujets aussi différents que les cahiers de

rappels ou l'usage des drones équipés de caméras pour surveiller le respect des mesures de confinement.

2. Nouvelles règles pour les cookies : un tournant pour les internautes et le secteur de la publicité en ligne

En publiant ses lignes directrices modificatives et sa recommandation le 1^{er} octobre 2020, la CNIL a rappelé deux règles fondamentales : l'internaute doit être informé, de façon claire et synthétique de ce à quoi servent les traceurs et il doit pouvoir refuser les cookies aussi facilement que les accepter.

Cette évolution des règles applicables a été accompagnée de la publication de nombreuses fiches pour les professionnels (mettre son site en conformité, les solutions pour outils de mesure d'audience, questions-réponses, etc.) et pour les particuliers (les changements au quotidien, les conseils pour maîtriser son navigateur, le logiciel CookieViz, etc.)

Le délai d'adaptation aux lignes directrices étant arrivé à son terme le 31 mars 2021, la CNIL s'assure désormais du respect de ces règles chez l'ensemble des acteurs publics et privés.

3. Une protection toujours plus forte des personnes dans leur quotidien numérique

En 2020, la CNIL a considérablement enrichi son offre éditoriale avec des fiches pratiques ou des conseils en lien avec l'actualité. Elle a mobilisé l'ensemble des moyens à sa disposition pour mieux communiquer auprès de ses différents publics sur les réseaux sociaux ou via son standard téléphonique.

Ainsi, près de 10 millions de visites ont été comptabilisées sur l'ensemble de ses sites web, soit une augmentation de 21 % par rapport à 2019, dont plus d'un million de consultations de la rubrique Besoin d'aide.

La CNIL a également reçu 13 585 plaintes soit 62,5 % d'augmentation depuis la mise en œuvre du RGPD. Ce chiffre, toujours élevé et constant par rapport à 2019, confirme une prise de conscience conséquente des Français vis-à-vis de leurs droits. Parmi ces plaintes, 4 528 ont été suivies d'une réponse rapide et 9 057 ont nécessité une étude plus approfondie.

La sécurité des données, une thématique prioritaire de contrôle pour la CNIL

La CNIL a reçu, en 2020, **2 825 notifications** de violation de données personnelles soit 24 % de plus qu'en 2019. Pour plus de 500 d'entre elles, l'origine est une attaque par rançongiciel, dont la CNIL a pu constater l'augmentation en 2020 et notoirement en 2021 pour des établissements de santé.

La CNIL sera particulièrement attentive, en 2021 et au-delà, au respect des règles de sécurité concernant les données de santé et dont la perte, l'altération ou l'accès non autorisé peuvent avoir des conséquences particulièrement importantes pour les personnes concernées.

Un renforcement de l'accompagnement et du conseil des professionnels et des pouvoirs publics

Si chaque organisme est responsable de sa conformité au RGPD et à la loi, la CNIL propose une boîte à outils complète pour les aider à comprendre et à appliquer les différentes règles. L'accompagnement des professionnels a été conduit à deux niveaux, avec des outils généraux et sectoriels.

Parmi les outils d'accompagnement généraux qu'elle destine aux professionnels, la CNIL a notamment publié un guide des tiers autorisés et un guide pour aider les professionnels à définir des durées de conservation, ainsi que de nombreux contenus sur les cookies et autres traceurs. D'autres

contenus, sur des outils de conformité prévus par le RGPD, ont également été mis à disposition des professionnels. De nouvelles fiches explicatives pour comprendre et maîtriser les codes de conduite (pour harmoniser des pratiques au niveau d'un secteur d'activité) ou des règles d'entreprise contraignantes (politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne), mais également la certification (d'un produit, service, processus ou système de données) sont ainsi disponibles sur cnil.fr.

La CNIL a également renforcé son accompagnement sectoriel en publiant de nouveaux référentiels, prenant en compte les exigences du RGPD, pour la gestion des cabinets médicaux et paramédicaux, pour la gestion des ressources humaines ainsi qu'une consultation sur un projet de référentiel pour la gestion locative.

Concernant les pouvoirs publics, la CNIL a participé à 20 auditions parlementaires et a répondu à 8 questionnaires adressés aux parlementaires. En 2020, elle a adopté 96 avis sur des projets de texte, notamment en lien avec la crise sanitaire ou concernant les fichiers PASP, GIPASP et EASP. Sans constituer une « autorisation » ou un « refus », ces avis permettent d'éclairer les pouvoirs publics sur des enjeux Informatique et Libertés.

De nombreux contrôles et des sanctions d'un montant total de 138 millions d'euros

En 2020, la CNIL a conduit 247 contrôles (82 en ligne, 74 sur pièces, 72 sur place et 19 auditions). Ces contrôles font suite à des plaintes/signalements (40 % des cas), sont effectués à l'initiative de la CNIL selon l'actualité (32 %) ou en lien avec les thématiques prioritaires annuelles (15 %) ou font suite à des mises en demeure ou des sanctions (3 %).

En 2020, la formation restreinte de la CNIL a prononcé 14 sanctions, dont 11 amendes d'un montant total de 138 489 300 euros (parfois accompagnées d'une injonction sous astreinte), 2 rappels à l'ordre et une injonction sous astreinte non associée à une amende. Un seul non-lieu a été prononcé.

Ces sanctions concernent des acteurs, des secteurs d'activités et des manquements très variés, et font notamment suite à une sécurité insuffisante des données ou à l'absence d'information et de consentement des personnes, en particulier concernant l'utilisation des cookies.

L'année aura également été marquée par une première sanction décidée en coopération avec les autres autorités de protection des données européennes dans le cadre de la procédure dite de « guichet unique ».

La présidente de la CNIL a par ailleurs prononcé 49 mises en demeure de se mettre en conformité, dont 3 publiques et 4 en coopération avec d'autres autorités de protection des données européennes. Elle a également prononcé 38 rappels à l'ordre et 2 avertissements, notamment suite à des plaintes.

Une coopération européenne intensifiée en 2020

Plus de 1 000 dossiers de coopération européenne concernaient des plaintes ou des contrôles. La CNIL a été autorité chef de file (quand l'établissement principal de l'organisme concerné se situe en France) dans une centaine de cas et autorité concernée dans près de 400 cas.

14 projets de sanctions européens ont été examinés par la CNIL, dont 6 décisions adoptées par la formation restreinte contenant des objections pertinentes et motivées ou des commentaires.

Une anticipation des enjeux pour la vie privée

Au-delà de ses missions d'accompagnement et de contrôle, la CNIL poursuit, au quotidien, son objectif d'anticipation de l'innovation technologique et de ses enjeux pour la vie privée et les libertés individuelles.

En 2020, la CNIL a notamment mené des réflexions sur le droit à la portabilité des données, avec un évènement organisé en novembre qui a contribué à la publication d'une nouvelle fiche pratique complète à l'attention des professionnels. Elle a également édité un premier livre blanc, À votre écoute, consacré aux assistants vocaux. En réponse à la mission éthique qui lui a été confiée par la loi pour une République numérique, la CNIL a également proposé un nouveau format pour son évènement annuel « air » (avenir, innovations, révolutions) sur le thème « les mutations dans le monde du travail ».

Un « bac à sable » pour un accompagnement spécifique

Dans le cadre de sa stratégie d'accompagnement, la CNIL a lancé une première session de « bac à sable données personnelles », sous la forme d'un appel à projet dans le domaine de la santé : douze projets bénéficieront ainsi en 2021 d'un accompagnement de la CNIL, dont quatre d'un accompagnement renforcé afin d'aboutir à une solution respectueuse de la vie privée des personnes.

Une anticipation des nouveaux usages du numérique après la crise sanitaire

Dans son rapport annuel, la CNIL présente des premières pistes de réflexion pour mieux comprendre les usages du numérique pendant les différents confinements et anticiper les innovations futures.

Un futur livre blanc sur les données de paiement

Les données de paiement, leur circulation et leur protection font partie intégrante des enjeux de société. En 2020, la pandémie a remis cette question sur le devant de la scène, en accélérant certaines transformations à l'œuvre dans le domaine des paiements. La CNIL entend aborder ce sujet de manière graduée et publiera prochainement un livre blanc sur le sujet.

Des travaux de recherche sur le profil des plaignants

Le 13 avril 2021, la CNIL a publié son 8e cahier Innovation et Prospective, Scènes de la vie numérique, consacré à la protection des données au quotidien par les individus. Cette publication explore la construction historique du droit autour de la protection des données personnelles, la diversité des pratiques individuelles en la matière, les situations sociales qui déterminent le recours à la CNIL et les étapes préalables à celui-ci.

Les données, un enjeu environnemental

Le réchauffement climatique et la transition environnementale sont au cœur des défis à relever, dès aujourd'hui et dans les années à venir. Le lien entre protection des données et environnement fera l'objet de travaux prospectifs du laboratoire d'innovation numérique de la CNIL (LINC) dès 2021.

GEORGIA / GEORGIE

State Inspector's Service

Major Developments in the Data Protection Field

November 2020 - May 2021

Introduction

As elsewhere, the global pandemic and related restrictive measures considerably affected personal data protection landscape in Georgia. During the state of emergency declared in the country to combat the spread of virus, rights to privacy and personal data protection were not substantially limited; however, due to restrictions on movement and personal communication, it became necessary to introduce new data processing procedures and/or move the existing processes online.

Despite the challenges emerged from Covid-19 crisis, limited human and infrastructural resources alongside legal and practical difficulties, Georgian Data Protection Authority - State Inspector's Service spared no effort to carry out its activities in personal data protection field.

In the mentioned period, the Service published a comprehensive report on its activities, which reviews not only the results and success achieved but also the factors that hindered accomplishment of the goals set by the Service. The report extensively compiles trends, challenges and achievements in 2020 as well as future plans of the Service.

MAJOR ACTIVITIES OF THE SERVICE IN THE FIELD OF DATA PROTECTION

Given the tasks and difficulties faced by the Service, its efforts were primarily aimed at prevention - raising awareness of public and those involved in pandemic management, as well as checking lawfulness of already implemented data processing procedures. Also, monitoring compliance of legal documents and electronic products developed during the pandemic with the Law of Georgia "on Personal Data Protection".

Although the Service has offered citizens several alternative ways for application (mobile app, website, email) against the backdrop of the pandemic, in 2020, the number of complaints on alleged cases of unlawful data processing decreased by 27%, in comparison to 2019 (422 in 2019, 305 in 2020); and as far as the Service inspects organisations both on the basis of citizens' complaints and on its own initiative, lack of complaints along with the restrictions imposed obviously affected the number of inspections carried out - it has decreased by 23% (156 in 2019, 119 in 2020).

In the reporting period, the Service introduced new preventive procedures, such as:

Self-Assessment Questionnaire - assisting public and private institutions to assess data protection processes within their entities. The questionnaire enables organisations, without the involvement of data protection authority, to assess processing operations themselves and identify risks and shortcomings, as well as define measures to be taken for data security.

Criteria to identify high-risk areas - The mentioned criteria (risk factors) identify areas where the probability of violating human rights and freedoms is high. Such criteria include: data processing in large volumes; processing special categories of data, data of vulnerable groups (including persons with disabilities) and data of minors by the organisation; use of innovative technologies in data processing, etc.

Considering the need to address pressing issues, among the priority areas has been: data processing in healthcare and financial sectors, in electronic databases; processing minors' data, etc.

Healthcare Sector

Due to the pandemic, the need for entirely new approaches arose in private and public entities. Many processes have moved online, new electronic products were introduced rapidly, which, in most cases, involved processing various types and large volumes of data. Sensitive (e.g. health-related) data were processed in unusual environments (trading facilities, hotels, etc.).

In view of the above, particular attention was paid to the most sensitive areas and the inspections were conducted in: medical institutions-so-called "fever clinics", "COVID clinics"; National Center for Disease Control and Public Health; hotel quarantine areas; National Tourism Administration (processing of data in quarantine/isolation through the website www.registration.gov.ge), shopping malls and airports (processing during temperature screening), etc.

For early detection and prevention of COVID-19 cases, at the initiative of the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs, a mobile (contact-tracing) application "Stop COVID" was introduced in the country. Taking into account the European countries' best practices, the Service prepared and submitted recommendations to the Ministry. The purpose of the recommendations was to bring data processing through the application in line with the law and gain public trust towards the application.

During this period, patients' data has not been widely disseminated without their or their family members' first-hand consent. Often, public figures themselves spread information that they have contracted the virus, which was conditioned by the public interest and/or high civic responsibility.

In order to promote high data protection standards, the Service arranged an online meeting with the multiple stakeholders from healthcare sector. The participants of the meeting discussed trends, challenges and future cooperation perspectives in relation to health-related data protection mechanisms. The meeting was followed by presentation of the compilation of the State Inspector's decisions concerning protection of health-related data.

In addition, Service examined legal acts regulating personal data processing during the pandemic. Among them were draft decrees, which regulated the management of the novel coronavirus (SARS-COV-2) infection (COVID-19), as well as processing and exchange of personal data (including special category data) by various agencies during the implementation of restrictions. The recommendations of the Service were mainly related to the following issues: setting and/or clearly defining data processing objectives; reducing the volume of personal data to be processed; determining data storage timeframes; regulating data deletion/ destruction rules and measures to be taken for data security.

Electronic Databases

As there is a growing trend of creating databases and technological development, the threats of unlawful data usage are also increasing. Accordingly, the efforts of the Service were also directed at improving the data processing procedures in the electronic databases.

In this regard, the Service developed a manual for developers of electronic systems/programs and applications, which aims to protect and secure personal data in electronic databases, as well as to ensure that the created product complies with the data protection legislation. Adherence to the rules set out in this document in the process of creating an electronic database will spare institutions from making changes to the already implemented product.

Furthermore, the Service conducted examination of legal documents that regulated data processing in electronic databases. The recommendations were mainly related to: defining and/or clearly indicating the objectives of data processing in electronic databases; determining the volume of data processing and storage timeframe, and creating a mechanism for deleting data after achieving the objective; as well as measures to be taken for ensuring data security.

Protecting Data of Minors

Protection of the right to privacy and personal data of minors remains a priority. Measures taken by the Service, on the one hand, were aimed at improving data processing in public and private institutions and raising awareness of those involved in the processing of children's data on a daily basis and, on the other hand, aimed to raise awareness of children and their parents.

The Service examined minors' data processing in public and private institutions where largescale and/or sensitive data of children are processed. For instance, inspections were conducted on the processing operations of: student data by the Office of Resource Officers of Educational Institutions through the unified electronic database (this database contains information on violations and/or alleged violations by 549,000 students in 607 public schools); students' personal files by public and private schools and the ongoing video surveillance in kindergarten/school buildings; patient data, video surveillance, audio monitoring and data security measures in medical institutions providing services to minors with mental disorders, as well as those who benefit from universal healthcare programs and receive vaccinations; and students' data during distance learning.

In order to promote effective protection of minors' data and their best interests, a number of activities were carried out. The Service organized high level meeting with the relevant organisations responsible for the protection of minors' data and discussed existing challenges along with cooperation mechanisms. The meeting was followed by presenting the compilation of the State Inspector's decisions concerning protection of minors' data.

A Memorandum of Understanding was concluded between the Service and Office of Resource Officers of Educational Institutions in order to improve the system of minors' personal data protection in the field of education. Within the framework of the MoU, the Service examined draft normative acts on their compliance with data protection legislation and developed relevant recommendations that were related to the protection of safety and public order in schools, as well as the rules on video surveillance and processing of video recording.

Moreover, the Service actively cooperated with the LEPL Education Management Information System in the process of certification of school principals, in particular, to address issues of data protection.

A recommendation has also been prepared for children and parents: "How to protect yourself from cyberbullying" (which aims to protect the personal data of minors on the internet) and on the very popular application "TIK TOK" in 2020 and the risks associated with it.

Additionally, for parents who apply to the Public Service Halls to register the birth of a child, the Service has placed information brochures in such facilities in 14 cities of Georgia. The brochures provide information on the importance of protecting children's personal data and the risks that may result from their misuse, dissemination, sharing and posting on social networks.

Data Processing in the Financial Sector

The COVID-19 pandemic has also affected activities of financial institutions and their clients. For example, under full lockdown, financial institutions intensified the use of biometric data (facial images) to remotely

identify a person. Thus, supervising lawfulness of data processing in the financial sector was one of the main directions of work of the Service.

The Service cooperated with the financial institutions, relevant sectoral associations and the supervisory body of financial institutions - the National Bank of Georgia. Meetings were held with the representatives of various financial institutions, including a webinar in cooperation with the Banking Association of Georgia, which about 100 representatives of commercial banks attended.

The Service actively cooperated with the Banking Association of Georgia on data processing issues in this sector, including the implementation of the concept of “Open Banking” in practice. “Open Banking” is the project initiated by the Banking Association of Georgia, within which information in financial institutions is immediately exchanged between various financial organisations by means of electronic technologies and on the initiative of user/client.

Occasionally, working meetings were held with the representatives of the National Bank of Georgia on various topical issues, including on data processing in the process of remote identification of clients and assessment of their solvency status.

The Service, within its competence, was also involved in the law-making process. In particular, the Service presented an opinion on the draft order of the Minister of Internal Affairs of Georgia, which was related to the creation of a special electronic program for registration of personal property received by the loan issuing entity (pawnshops) as a means of securing requested amount of loan;

Awareness Raising Activities

One of the main direction of activities of the Service is raising awareness of public on personal data protection issues in Georgia. Therefore, the Service continuously prioritizes this area and conducts a great deal of activities in this regard annually.

Data Protection Day

Late in January, 2021 the Service announced launch of the week of events marking an International Data Protection Day in Georgia and plenty of activities were carried out to celebrate this day, including:

Essay Competition and Online Student Conference was carried out in cooperation with one of the Universities of Georgia. Students of all higher education institutions were invited to participate and present an essay on the selected topics in it. The following topics were selected for the essay: Protection of personal data of schoolchildren and students during distance learning, threats of sharing minors’ personal data on the Internet, impact of COVID-19 pandemic on data processing, protection of personal data in online services, protection of minors’ data and data security. About 60 students took part in it and at the end of the competition, an online conference was organized with the participation of the winning contestants. The printed version of successful participants’ essays will be published, while the top three students are currently undergoing a two-month internship in the Service.

After a while, this event was followed by the presentation of the collection of students’ articles on - “Pressing Issues and Challenges related to Personal Data Protection”. The collection combines 12 papers prepared by the students from the different higher educational institutions within the framework of the essay contest by the Service. The papers cover pressing issues such as: protection of students’ data in the process of distance learning; protection of health data during the COVID-19 pandemic; data protection in online services during the pandemic; and threats of sharing minors’ data on the Internet. At the end of the event, the successful participants of the Essay Contest were awarded certificates.

Photo Contest for pupils- “My Personal Data is Mine” was also conducted and the winners awarded. The goal of the project was to instill interest in the young generation and share their vision on data

protection issues. Around 100 schoolchildren participated in the contest from different regions of Georgia. The children presented threats that resulted in improper protection of data, from their perspective.

A Workshop was organized by the Service and the representatives of public, private and non-governmental organisations, working in data protection area, were invited to participate. The attendees were informed on the activities of the Service as well as the trends and existing challenges in the country. Future cooperation mechanisms were also discussed during the meeting.

Informational meetings in capital city and regions of Georgia were also organised within the Service's project of "Data Protection Ambassadors". During the meetings young Ambassadors informed interested members from general public about the functions of the Service, importance of data protection and other related issues.

Apart from above, on 28 January, 2021, the State Inspector published special announcement, where the importance of data protection in modern technological era and the need for cooperation in this regard was highlighted.

Trainings and learning courses of the Service

E-learning Portal - the Service developed its first distance learning portal where sector-specific training modules are integrated. The first module introduced was a long term distance learning course - on the protection of personal data in healthcare sector. The course is specifically designed for this sector with due respect to its specificities. It aims at ensuring high standard of data protection in the healthcare sector and at eradicating existing shortcomings. The Service periodically will add other courses designed for relevant sectors on the portal.

Cooperation with training and professional development centers - The reporting period was also active in terms of cooperation with training and professional development centers of public agencies. Workshops were organised with the aim to plan joint projects and increase coordination. These meetings were preceded by an analysis conducted by the Service, which revealed the need to strengthen efforts to raise the qualification and awareness of public officials on data protection issues. In response to the challenges, an agreement was reached with the participants on issues such as: the introduction of special preparatory courses for data protection, updating of existing curricula, continuous in-service training of public servants, strengthening trainers' resources and implementation of joint educational projects.

TOT for directors and teachers – the training of trainers on data protection was conducted in cooperation with the Public Defender (Ombudsman) and the Ministry of Education and Science of Georgia. The objective of the training is to improve the teachers' and directors' of general educational institutions capacity in Human Right issues. The distance learning was conducted in two stages and covered more than 150 participants.

Strengthening PDP standards in Law Enforcement Sector- the Service conducted a training on data protection issues for the staff of the Department of Human Rights Protection and Investigation Quality Monitoring and Main Division of Juvenile Division under the Tbilisi Police Department of the Ministry of Internal Affairs. The training course was aimed at drawing attention of persons responsible for the monitoring of the investigative process on data protection topics and increasing quality of protection of juveniles' data in investigative process by the investigators specialized in juvenile cases.

HELP course for LEA - HELP distance learning course on Data Protection and Privacy Rights, launched during the previous reporting period, has been successfully implemented in collaboration with the Council of Europe. The aim of this learning course was to raise the awareness of law enforcement agencies, improve privacy and data protection standards in this sector. It underwent several months of intensive training and more than 30 representatives from the Prosecutor's Office, the Ministry of Internal Affairs and

the Ministry of Defense, the Special Penitentiary Service, the State Security Service and the Investigation Service of the Ministry of Finance of Georgia were participating in the training.

Personal Data Protection Ambassadors – of the Service underwent a three-day enhanced training course. The course aimed at preparing the participants theoretically and improve their practical skills. Consequently, young ambassadors will more actively engage in public awareness-raising process across the country and provide citizens with information about their rights. The Service launched the “Personal Data Protection Ambassadors” project in 2020 and continues its successful implementation. The purpose of the project is to support students’ development and raise public awareness on personal data protection issues.

Trainings for the staff - It shall also be noted that along with the awareness raising activities aimed to the target groups and public in general, the Service also took care to strengthen the capacity of its staff during the pandemic. In 2020, 33 training activities were conducted for the staff of the State Inspector’s Service, during which more than 370 trainees underwent the training. In order to align national data protection legislation and practices with modern European standards, the staff of the Service was trained on the topics of General Data Protection Regulation (GDPR) and European data protection standards. Taking into account the challenges posed by the development of modern technology, employees have been trained on the issues of artificial intelligence and personal data protection.

Cooperation with NGOs and other State Institutions

In order to enhance cooperation with non-governmental sector, the Service continues initiation of the meetings with them. During the reporting period, the State Inspector held a meeting with the representatives of NGOs. The goal of the meeting was introducing main achievements, implemented reforms and challenges. Particular attention was paid to the practical and legislative challenges that the Service faces in its practice.

With the joint initiative of the Service and the local NGO a new project, “Supporting Personal Data Protection in Georgia” was launched. In the framework of the project, special attention will be paid to raising public awareness and promoting development of younger generation. Additionally, the project will foster discussions on challenges related to data protection in the relevant professional groups and academia. The project activities also include preparing researches, thematic publications, booklets and video clips. The special needs of persons with disabilities will be considered as well.

During the mentioned period, the Service concluded a bilateral memorandum of understanding with Georgian Association of Mediators. The memorandum aims to establish high standards of data protection in the field of mediation and to develop cooperation between the institutions in this direction. The parties of the MoU will cooperate in the direction of preparing legal documents that regulate data processing in the mediation process, raising mediators’ awareness on data protection issues and providing legal consultations on data processing in practical activities of mediators.

International Cooperation

During the reporting period the Service continued its active participation in various international formats on behalf of the country.

The Service participated in the International Forum on Privacy and Data Protection (IFPDP) and delivered a speech. During the speech the state of protection of personal data in Georgia was assessed and discussed existing legislative regulations, steps taken towards data protection in Georgia by the Service, as well as possibilities and challenges in this area.

As an organizing agency, the Service participated in the working group - the spring Conference of European Data Protection Authorities. The Service also actively participated in sittings organized and various working groups set up by Global Privacy Assembly. The representatives of the Service work on important issues such as: digital technologies, artificial intelligence, data protection rights and other topical directions.

As the Service became a representative of Georgia at the Ad hoc Committee on Artificial Intelligence (CAHAI), the 3rd and 4th meetings of the Committee were attended by the representative of the Service *(Hereby, it shall be noted that, for the first time in the history of the Georgian Internet Governance Forum, the Service spoke about the importance of personal data protection in the development of technologies and artificial intelligence. Emphasis was put on the significance of personal data protection, right to privacy and other democratic values when introducing and using artificial intelligence-based technologies, inter alia, the support for regulation and development in this area. The event was attended by about 100 participants in an online format (the video posted on the official Facebook page of the Service accumulated 10,100 views)).*

It should be emphasized that the Service continues to actively support speeding up the process of signing the 108+ Convention by Georgia, which will significantly contribute to the approximation of national data protection legislation to international standards after its entry into force. The Service expresses hope that the country will sign the Second Additional Protocol of the Convention in 2021.

HUNGARY / HONGRIE

Major developments in the data protection field in Hungary since November 2020

President of the Authority

Although the term of office of the President of the Hungarian National Authority for Data Protection and Freedom of Information expired at the end of 2020, Dr. Attila Péterfalvi was re-elected for another 9 years.

Data protection measures in connection with the fight against Covid-19

The Authority prepared a number of documents to inform stakeholders about the data protection challenges of the fight against the COVID-19 pandemic which were published on the www.naih.hu website.

For example:

- **Information on the data protection and data security aspects of digital distance learning**

The extracurricular digital education introduced during the first wave of the Covid-19 pandemic gave rise to a number of data protection and data security issues, particularly in relation to the uploading, sharing and storage of teaching materials, video recordings that verify completion of the students' tasks and other documents. The Hungarian National Authority for Data Protection and Freedom of Information regarded the elevation of data protection awareness as a task of outstanding importance by way of statements published in its website among the institutions as well as the teachers, educators, speakers, trainers and parents in this field. Because of the rapid proliferation of the pandemic during its second wave, increasing numbers of educational institutions decided to introduce digital education again so the Authority issued information concerning the data protection and data security aspects of digital distance teaching.

- **Guidance concerning certain data processing operations related to the measurement of body temperature during the period of epidemiological readiness introduced with ordering a health emergency in view of the novel coronavirus pandemic (Covid-19)**

Projects:

- **STAR II Project**

Financed by the European Union, the STAR II (Support small And medium enterprises on the data protection Reform II) project, ran – among others – in the partnership of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) had the aim of assisting SMEs in applying the GDPR.

Taking the structure and needs of SMEs into account, the project helps the enterprises in question shape an appropriate practice.

In the course of the project, partners survey how the EU data protection authorities call, and have called, the attention of SMEs to their obligations arising from GDPR, and also gather information on the experience gained by SMEs in applying the GDPR.

In order to interact with SMEs, assist them to ensure compliance with the GDPR and gather valuable information about the difficulties they face, NAIH was operating a hotline for SMEs between 2019 and

2020. During this period the kkvhotline@naih.hu of the NAIH provided information for SMEs throughout the European Union in respect of the interpretation and proper application of the GDPR.

On the basis of the questions and issues raised by the SMEs, a handbook has been compiled which is accessible and usable throughout the EU. This Handbook helps SMEs to comply with their legal obligations and explains some of the main features of the GDPR in simple language. It also provides cases and practical examples to guide SMEs.

- **KÖFOP-2.2.6-VEKOP-18-2019-00001 special project "Exploring local practices of freedom of information and increasing their effectiveness"**

The Hungarian National Authority for Data Protection and Freedom of Information has been awarded a non-reimbursable EU grant worth HUF 1 billion to implement the KÖFOP-2.2.6-VEKOP-18-2019-00001 special project "Exploring local practices of freedom of information and increasing their effectiveness". The objective of the project is to investigate the implementation of freedom of information practices in Hungary through applied research and to develop the necessary proposals for optimisation.

In addition to the protection of personal data, the Hungarian National Authority for Data Protection and Freedom of Information is responsible for the implementation of the freedom of information as a fundamental right. A comprehensive review of decades of practice in Hungary is essential in order to uncover the factors that hinder the exercise of this right. Once they have been identified, targeted proposals can be made to optimise the disclosure of information in the public interest.

INDONESIA / INDONÉSIE

Indonesia has aimed to improve its regulatory framework and practice on personal data protection. The Indonesian government is changing the personal data protection system from a sectoral-based approach to a comprehensive system. Act 11/2008, as amended by Act 19/2016 and Government Regulation (GR) 71/2019, as the implementing regulation, have started the changing process. GR 71/2019 stipulates legal bases and principles in processing personal data; both are adopted from GDPR.

Furthermore, the government and the parliament of Indonesia have been discussing Personal Data Protection Bill since early 2020. The discussion is another progressive step that Indonesia has taken to develop its regime on personal data protection. Personal data protection is considered as part of the constitutional rights of Indonesian citizens. The bill also adopts fundamental elements of the GDPR. This law will regulate the legal bases in processing personal data, principles in processing personal data, rights of data subjects, and obligations of data controllers and data processors. The Bill also regulates the transfer of personal data, government roles, dispute resolution and procedural law, and administrative and penal sanctions. PDP Bill applies to both private and government sectors. Thus, it will become a comprehensive legal umbrella regarding how personal data should be regulated and protected in Indonesia. Indonesia expects the Bill will be passed into law this year.

ITALY / ITALIE

Major developments in the data protection field

(November 2020- June 2021)

Covid-19

The Garante has continued intervening on the processing of personal data related to the containment of the pandemic also in the considered period.

In January 2021 a favourable opinion was adopted on the draft act which regulates the organization and functioning of the national telephone and telematic support service for people who tested positive for Covid-19. On that occasion, the Authority considered that the identification of whoever calls the call center his/her positive status should take place through a specific code, which uniquely identifies the single report and the person associated with it, instead of using other less secure methods and avoiding the creation of a new database of Covid reports. The Garante also requested that the platform used by the call center operators to access the Health Card System be designed and implemented by adopting stringent security measures appropriate to the risk that such delicate data processing presents. Finally, the Authority required the Ministry of Health to carry out constant checks on the activity of the person entrusted with the management of the call center, to verify full compliance with the privacy regulations. In light of the innovations introduced with the establishment of the call center, the Ministry will also have to update the impact assessment relating to the data processing carried out under the Covid-19 alert system.

In February 2021 the Italian DPA issued FAQs on the processing of personal data related to vaccination at workplace. With such document, the Authority aimed at providing useful information to companies, organizations and public bodies so that they can improve data protection measures in the emergency context, also in order to prevent possible unlawful processing of personal data and to avoid unnecessary management costs or possible discriminatory effects. In the FAQs it is explained that the employer cannot acquire, even with the consent of the employee or through the competent doctor, the names of vaccinated personnel or copies of vaccination certificates. The employee's consent cannot constitute, in these cases, a lawful pre-requisite for data processing. The Garante also clarified that - pending an intervention by the national legislator that possibly imposes vaccination against Covid-19 as a condition for the performance of certain professions, work activities and duties in cases of direct exposure to "biological agents" during the work, as in the health context, the provisions in force on the "protective measures" envisaged for such work environments apply. Even in these cases, only the competent doctor, in his/her function of connection between the health system and the working context, can process personal data relating to employee vaccination.

Processing related to vaccination in the workplace was also the object of a policy document adopted by the Garante in May 2021, pending a definitive regulatory framework. The Garante specified that the main data processing activities - from the collection of subscriptions, to the administration, to the registration in the regional systems of the vaccination - must be carried out by the competent doctor or other identified health personnel. Within the framework of the rules protecting the dignity and freedom of data subjects in the workplace, the employer is not allowed to collect information directly from employees, the competent doctor or other health professionals relating to the intention to adhere to the campaign or to the administration (or not) of the vaccine and other data relating to his/her health conditions. Taking into account the imbalance in the relationship between employer and employee, the consent of the worker cannot in these cases constitute a valid prerequisite for processing vaccination data, just as it is not allowed to derive any consequence, neither positive nor negative, from the adhesion or not to the vaccination campaign.

In March 2021, with the arrival of the anti-Covid-19 vaccines, a further discussion has developed on the opportunity to start implementing solutions, including digital ones (e.g. apps), to respond to the need to make information on being vaccinated or not as a condition for access to certain premises or for the use of

certain services (e.g. airports, hotels, stations, gyms, etc.). In this regard, the Garante has drawn the attention of policy makers and private operators to the obligation to comply with the regulations on the protection of personal data, in particular on the protection of particularly sensitive data (those relating to the vaccination status) whose incorrect processing can cause very serious consequences for the life and fundamental rights of people. The Garante highlighted that the processing of data relating to the vaccination status of citizens for the purpose of accessing certain premises or the use of certain services, must be the subject of a national law, in compliance with the principles on the protection of personal data (in particular, those of proportionality, purpose limitation and data minimization), in order to achieve a fair balance between the public interest to be pursued and the individual right to privacy.

In May 2021 the Garante intervened on the decree that was adopted by the Italian government introducing the so-called 'green pass', or vaccination pass, which revealed criticalities such as to undermine – in the absence of the required amendments – the soundness of the arrangements to lift travelling bans during the pandemic. Therefore urgent measures have been accordingly required to protect rights and freedoms of natural persons.

On that occasion, the Garante highlighted that the so-called 'Italy Reopens' decree did not provide a suitable legal basis to introduce and regulate a nationwide green pass and was affected by data protection shortcomings including the lack of any assessment of possible large-scale risks for the rights and freedoms of individuals.

It highlighted that the law should specify the purposes of the processing of health data and avoid multifarious, unforeseeable future applications that are potentially in conflict with similar EU-wide initiatives, allow the definition of the controller of the processing at issue, to facilitate the exercise of data subjects' rights, ensure that only pertinent and accurate personal data are included in the pass, which must be produced in case of controls – in due respect of the data minimization principle and limited retention periods.

In June 2021 the Garante ordered the temporary blocking of the processing of personal data against the company that manages an application which was used for the first time to allow spectators in possession of certification certifying vaccination, recovery or negativity from Covid-19 to enter the Italian Cup final. The measure became necessary as the possibility emerged that the app could be used to govern access to other events and shows or other sporting initiatives. The Garante underlined that at the moment there was no valid legal basis for the processing of data, even particularly delicate ones such as those of a health nature, carried out through the app and aimed at ascertaining the "Covid free" situation of those who participate to sporting events as well as to other public events or access premises open to the public. The company should have refrained from any data processing since the time provided for the taking of a decision by the Authority had not elapsed.

Public sector

In November 2020 the Garante issued an opinion on the measures to be adopted by the national body which coordinates insurance funds (INPS) to obtain (also through appropriate agreements with other public bodies) the necessary data to carry out checks on the allocation of the minimum income guaranteed by the State. The processing of data that INPS would carry out, despite being aimed at the execution of a task of public interest, present high risks for the rights and freedoms of the data subjects as they involve exchanges of personal data - on a large scale and with telematic methods - relating to health, social condition and economic and financial situation, as well as criminal convictions and offenses, mainly referring to vulnerable subjects, including minors.

On that opinion, the Garante highlighted that the data exchanged between INPS and the various administrations – including Tax Registry, Regions, Municipalities - must be limited to those strictly necessary to carry out the checks required by law (e.g. possession of real estate, registration of vehicles, admission to long-term public facilities, convictions or personal precautionary measures).

Furthermore, adequate security measures must be adopted to ensure the integrity and confidentiality of the data both with reference to the information flows (for example, by means of techniques capable of ensuring the encryption of information and the digital signature) and with reference to the processing

carried out by the administrations that hold the data (which will be able to process the data of the beneficiaries transmitted by INPS only for the time necessary to carry out the checks).

Telecommunications

Further to a complex proceeding that the Garante had initiated following hundreds of complaints and alerts submitted by users against unsolicited phone calls, the Authority ordered a telephone company to pay a fine of more than Euro 12,250,000 for having unlawfully processed the personal data of millions of users for telemarketing purposes. The company was also required to implement several measures set out by the Garante in order to comply with national and EU data protection legislation, including on consent requirements, other key principles such as accountability, data protection by design, security measures on customer resource management.

Cookies

In December 2020 a public consultation on the rules for the use of cookies and other tracking tools by web sites has been launched by the Italian Data Protection Authority. More precisely, the guidelines issued by the Garante and submitted to consultation include, amongst others, some indications relating to “passive” tracking systems (such as fingerprinting), to “scrolling”, to the repetition of requests for consent from users, to third-party cookies. The consultation – addressed to entrepreneurs, consumers and operators - aims to acquire observations and proposals on the indications contained in the Guidelines.

Social Network

In January 2021, the Garante imposed an immediate limitation on the processing performed by TikTok - the social network that is particularly popular among children to create, share and comment short videos - with regard to the data of users whose age could not be established with certainty. The Authority decided to take urgent measures following the dismay caused by the death of a 10-year girl. In December 2020, the Garante had already notified TikTok several infringements including poor attention to the protection of minors, the easy dodging of the registration ban the company applies to children under 13 years, non-transparent and unclear information provided to users, and default settings falling short of privacy requirements. Pending receipt of the feedback that was requested via the above notification, the Garante decided to anyhow step in order to afford immediate protection to the minors in Italy that have joined the social platform. This is why the Italian SA banned TikTok from further processing the data relating to any user ‘whose age could not be established with full certainty so as to ensure compliance with the age-related requirements’. Following the intervention of the Italian DPA Tik Tok has announced the intention to adopt measures to limit to block access to users under the age of 13, to evaluate the use of artificial intelligence systems for age verification and to launch an information campaign to raise awareness among parents and children.

Deepfake

In December 2020, the Authority developed an information sheet to make users aware of the risks associated with the malevolent uses of deep fakes, photos, videos and audio created thanks to artificial intelligence (AI) software which, starting from real contents (images and audio), are able to modify or recreate, in an extremely realistic way, the characteristics and movements of a face or a body and to faithfully imitate a certain voice. The document aims at providing some tips on how individuals can protect themselves from Deepfakes.

Videosurveillance

In December 2020, new Frequently Asked Questions (FAQs) have been adopted by the Garante on issues concerning the processing of personal data in the context of the installation of video surveillance systems by public and private entities. The clarifications were necessary due to the new provisions introduced by Regulation 2016/679, in the light of which the validity of the indications already provided by the Garante on the matter in 2010 had to be assessed. The FAQs also take into account the Guidelines adopted on the subject of video surveillance by the European Data Protection Board (EDPB) and contain a simplified disclosure model drawn up precisely on the basis of the example proposed by the EDPB.

Data theft

In April 2021, after the data – including phone numbers and email accounts – relating to about 36 million Italians landed online following a breach into Facebook's systems, the Garante requested Facebook to take measures to limit data theft risks and to immediately offer a service enabling all Italian users to check whether their phone numbers or email accounts were affected by the breach. Indeed, the phone number might be exploited in such a case for various unlawful purposes ranging from unsolicited calls or messages to serious threats like the so-called 'SIM swapping' – i.e., an attack technique where the legitimate owner's phone number is used to breach into online services that rely exactly on one's phone number for authentication purposes.

The Garante reminded any party holding the personal data derived from the breach that the use of such data for whatever purpose is prohibited by data protection law as the information in question results from unlawful processing activities.

The Garante also drew the affected users' attention to the need for being especially vigilant in the coming weeks and provided specific indications on unusual events in the operation of their phones that could reveal fraud attempts.

The Garante also launched an investigation against LinkedIn following the violation of the social network systems which led to the dissemination of users' data, including IDs, full names, email addresses, telephone numbers, connections to other profiles and those of other social media, professional titles and other work information entered in their profiles by users.

As in the previous case, the Authority warned anyone who had come into possession of personal data deriving from the violation that their possible use is in contrast with the legislation on the protection of personal data, since such information is the result of unlawful processing and called all users affected by the violation to pay particular attention to any anomalies related to their telephone number or account.

Privacy information via icons

In March 2021, the Garante launched a contest calling for creative solutions that can make data protection information notices to data subjects simpler, clearer and immediately understandable through icons, symbols or other graphic elements, to make sure that the notices are really helpful and suitable for the purpose for which they are intended. As the information notices used by companies, web operators, public bodies, are often lengthy and complex, the Garante has called upon software developers, tech professionals, experts, lawyers, designers, university students, and anyone interested in this topic, to send a set of symbols or icons that can efficiently represent all the items that must be contained in an information notice under Articles 13 and 14 of the GDPR.

The right to privacy in prisons

In April 2021, following several reports relating to episodes in which video calls and interviews via Skype of people detained in prison would take place in the absence of the necessary minimum conditions of confidentiality and, in particular, in violation of the prohibition of auditory control by the custodial staff, the Garante and the Authority for the rights of persons deprived of personal liberty have jointly recalled the Directorates of Prisons and the operators responsible for respecting some essential guarantees for the protection of the confidentiality of prisoners who access this mode communication or interview. The two authorities have recommended, without prejudice to any measures ordered by the judicial authority, to prepare the connection spots in such a way as to allow the custody staff to visually control the interview from a distance, approaching the screen only to proceed with the necessary operations to identify the interlocutors, without however listening to the conversation; they have recommended that the identity of the correspondent be ascertained at the beginning and at the end of the conversation with the timely abandonment of the communication environment to ensure the confidentiality of the conversation.

Further to the joint statement, the Presidents of the two Authorities have signed a memorandum of understanding on the protection of individuals deprived of personal liberty. The two Authorities will cooperate to protect the dignity and rights of prisoners and other persons subjected to forms of limitation of freedom, such as migrants detained in CPR (Repatriation Centers) and the guests of the REMS (Residences for the execution of security measures). They will be able to activate joint inspections and investigations on cases of mutual interest, launch fact-finding investigations, exchange information on possible violations pertaining to the other Authority.

INTER-AMERICAN INSTITUTE OF HUMAN RIGHTS (IHR) / INSTITUT INTER-AMERICAIN DES DROITS DE L'HOMME

Inter-american Institute of Human Rights (IHR) is launching the FIRST course on data protection and human rights.



The IHR, through its Regional Office for South America, invites legal professionals or other careers, with a minimum of four years of higher education, to apply for the I Inter-American Diploma "The Human Right to Privacy and Protection of Personal Data ". The general objective of the Diploma is for the graduate to acquire specific legal knowledge on the main aspects related to the protection of personal data in accordance with national and international regulations from a perspective of protection of human rights.

The Diploma will take place from June 28 to August 13, 2021, virtually through the Aula Virtual Interamericana (AVI) and Zoom platforms. The first week will be dedicated to an induction on the use of the AVI

Director: Eduardo Bertoni, Alternate Representative and Coordinator of the IHR Regional Office for South America

To see all the information, [click here](#)

El IIDH por medio de su Oficina Regional para América del Sur invita a profesionales del Derecho u otras carreras, con un mínimo de cuatro años de estudios superiores, a postularse al I Diplomado Interamericano "El Derecho Humano a la Privacidad y la Protección de Datos Personales".

El objetivo general del Diplomado consiste en que la persona egresada adquiera conocimientos jurídicos específicos sobre los principales aspectos referidos a la protección de datos personales de acuerdo con la normativa nacional e internacional desde una perspectiva de protección de los derechos humanos.

El Diplomado tendrá lugar del 28 de junio al 13 de agosto de 2021, de manera virtual mediante las plataformas del Aula Virtual Interamericana (AVI) y Zoom. La primera semana se dedicará a la inducción sobre el uso del AVI.

Director: [Eduardo Bertoni](#), representante alterno y coordinador de la Oficina Regional del IIDH para América del Sur

Para ver toda la información, haga clic [aquí](#).

JAPAN / JAPON

1. 2020 Amendment of the Act on the Protection of Personal Information

The Amended Act on the Protection of Personal Information (hereafter referred as the amended APPI) was promulgated on 12th June 2020. The amended APPI, except for some parts, will come into force on 1st April 2022.

The amendments were primarily made to achieve the following purposes;

- To develop necessary and sufficient measures to protect the rights and interests of individuals in light of increased awareness among individuals regarding their own personal information,
- To ensure a system where the benefits of technological innovation are shared by both economic growth etc. and the protection of the rights and interests of individuals,
- To establish a system that takes into account the diversity of risks faced by individuals, and international harmonization and collaboration as a variety of services that use personal information are being developed globally, and
- To develop an environment where personal information is being used appropriately within the foreseeable scope by an individual, while business operators are able to explain their responsibilities in relation to the rights and interests of the individual as use of personal information becomes more diverse due to the progress of technological innovation.

Broadly speaking, the amendments were made with regard to the following 6 perspectives; (1) individual rights, (2) obligations that business operators should abide by, (3) frameworks to encourage voluntary activities of business operators, (4) policies for data utilization, (5) penalties, and (6) extraterritorial application of APPI and cross-border transfer of data. The Overview of the Amended APPI (Annex 1) and the Comparative table of the current and the amended provisions of the APPI (Annex 2), both of them were already being shared with the European Commission, are herewith included for your reference.

For more information of the amended APPI, please see the following links:

Overview of the amended APPI : https://www.ppc.go.jp/files/pdf/overview_amended_act.pdf

Comparative time table of the amended

APPI : https://www.ppc.go.jp/files/pdf/20200612_comparative_table_amended_APPI.pdf

(Note: The above mentioned part of the revision of the APPI was made prior to November 2020. However, the PPC Japan would like to inform this development in this part of the update.)

2. 2021 Amendment of the Act on the Protection of Personal Information

The amendment act that includes the amendment to consolidate three laws, the Act on the Protection of Personal Information (APPI), the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO), and the Act on the Protection of Personal Information Held by incorporated Administrative Agencies, etc. (APPIHAA), into one single legislation was approved by the Diet on 12th May 2021 and promulgated on 19th May 2021.

The provisions on national government and incorporated administrative agencies etc., and the revision of the exemption provision for academic research institutions etc. will be enforced within one year after the promulgation, and the provisions on local government and local incorporated administrative agencies etc. will be enforced within 2 years from the promulgation. The following changes are to be made:

- (1) In addition to integrating the three laws of the APPI, the APPIHAO, and the APPIHAA, etc. into one law, it stipulates common nationwide rules for local governments' personal information protection systems and unifies the entire jurisdiction under the Personal Information Protection Commission.
- (2) In principle, the same rules apply to both public and private hospitals and universities, etc. in order to unify regulations in medical and academic fields.
- (3) Review across-the-board exemption provisions on academic researches under the current APPI, and exemption provisions to several obligations will be put in place.
- (4) Standardize the definition of personal information, etc. in the national government, private sector, and local governments, and clarify the rules regarding the handling of anonymously-processed information by government agencies, etc.

INTERNATIONAL COMMITTEE OF THE RED CROSS / COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (ICRC)

- **The DigitHarium**

In January we launched the [DigitHarium](#), a one year initiative, a global forum to discuss and debate digital transformation within the humanitarian sector, with a focus on humanitarian protection, policy, ethics and action.

The DigitHarium provides a space where humanitarian, diplomatic, academic and technology practitioners can meet to collaborate in order to find local and global solutions to today's digital dilemmas.

Humanitarian digital transformation is about putting people first, with technology forming part of the solution to specific humanitarian issues. The needs and aspirations of people who need humanitarian assistance should guide humanitarian action. Similarly, the impact of humanitarian digital solutions and cyber activities on people in need should be monitored and addressed.

The humanitarian data ecosystem is interconnected and no one organization can tackle these challenges single-handedly. The DigitHarium brings together practitioners from different fields, with a range of experience, to build a community of practice that analyses these challenges and develops practicable solutions.

Every month, the DigitHarium will discuss a new theme, examining the implications for humanitarian action and exploring solutions. The monthly theme will be discussed through three main channels:

- a monthly Digital Dilemmas Dialogue: a 30-minute discussion between two experts;
- a monthly Digital Dilemmas Debate: a 60-minute roundtable with a panel of experts, practitioners and other stakeholder groups;
- regular blog articles and podcasts offering a range of perspectives.

Participants, so far, have included, among many others: Joe Cannataci (UN Special Rapporteur on the Right to Privacy), Wojciech Wiewiórowski (the European Data Protection Supervisor), and Immaculate Cassait (Kenya Data Commissioner).

The month of June will focus on Connectivity as Aid, Connectivity for Aid, and Internet Shutdowns and will feature among many activities a discussion between the President of the ICRC, Peter Maurer, and the Minister of Development and Humanitarian Affairs and Economy, H.E. Franz Fayot.

- **Handbook on Data Protection in Humanitarian Action, Second Edition**

The Handbook has already been presented numerous times to the TPD. In 2021 the Handbook has been translated also into French, and Spanish. Additional language versions are expected to be released this year: Russian, Arabic, and Japanese.

All language versions are/will be available here: <https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action-pdf-en-2>

More background is available here: <https://www.icrc.org/en/data-protection-humanitarian-action-handbook>

LIECHTENSTEIN

Signature of Convention 108+

Following approval by the government, the Principality of Liechtenstein signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) on December 7, 2020. Currently, documentation is being prepared for the debate in Parliament to approve further ratification of the Protocol.

MALTA / MALTE

Insofar as legislative interventions are concerned, during the year under review, a legal notice was brought into force, by means of which the processing of data concerning health for insurance business purposes was further regulated. The regulations brought about by means of this amending legal notice – Legal Notice 107 of 2020 - set out further conditions and clarity on the processing of such data.

This Office sustained its efforts to promulgate data protection awareness for the benefit of the general public and more specifically controllers operating within different sectors and therefore to as wide an audience as possible, in order to ensure a general level of awareness is imparted across the board. In this regard, the Office applied for European Funds and submitted a proposal to the European Commission for a funded project specifically designed to raise data protection awareness among data subjects and assist small and medium enterprises, in particular start-ups, to ensure compliance with data protection rules deriving from the General Data Protection Regulation. This project, as granted, has a duration of twenty four months and is phased in three distinct work packages consisting in:

- Multi-level Awareness Raising Campaign, targeting the general public to inform them of their rights under the GDPR;
- Development of a Compliance tool, to facilitate compliance by Small to Medium Enterprises and Data Protection Officers;
- Dissemination and exploitation tool, through conferences and seminars across Malta and Gozo

Furthermore the Office continued to renovate its portal and enhanced its online platform by means of which data subjects can easily lodge a complaint for action by this Office in those cases where they believe that their data protection rights have been infringed. In addition, important tools within the portal were enhanced, including specific sections intended to guide controllers to notify data breaches and conduct data protection impact assessments. A new FAQs section was developed whereby the most frequently asked enquiries can be found. Both individuals and institutions can benefit from this section as the information is tantamount to a practical guide on everyday matters such as the reporting of data breaches, the handling of research data, retention periods and the uses of CCTV cameras.

During the year under review, the office received a total of 239 general consultation enquiries. The matters enquired most frequently about include data subject rights, CCTV cameras, retention period of personal data, direct marketing rules and restrictions on international transfers, among others.

Insofar as complaints are concerned, a total of 447 were received. Out of these complaints, 113 were either deemed to be inadmissible at a preliminary stage or else withdrawn or abandoned by the data subject at a later stage during the course of the investigation. The remaining 334 admissible complaints were investigated and 66 of them resulted in an infringement of the data protection legislation.

MAURITIUS / MAURICE

1. Data Protection Day 2021

The office promoted the Data Protection Day 2021 by publishing on its website a video containing useful information on this day and best practices for individuals and organisations which is available at the following link:

<https://dataprotection.govmu.org/Video%20Gallery/SiteAssets/Data%20Protection%20Day%202021.mp4?csf=1&e=D5nzcl>

The video was also circulated to all government officers and to the Mauritius Broadcasting Corporation (MBC) to broadcast in the news bulletin of 28/01/2021. Furthermore, the Data Protection Commissioner was interviewed by MBC radio regarding the role of the Data Protection Office, its mandate, ratification of Convention 108 +, EU Adequacy and the enforcement of the Act.

2. Publication of a guideline on National Security and Privacy

This guide examines the privacy implications of national security projects with the DPA and elaborates on the legal provisions on national security. The guide also sets out a number of recommendations to state authorities on the promotion of privacy compliance practices in the implementation of projects of national security interests.

3. Sensitisation

The Commissioner participated as guest speaker/panelist in various forums/Seminars such as the Audit Committee Forum (ACF) organised by the Mauritius Institute of Directors (MloD) and KPMG, Seminar themed 'Novembre Numérique' organised by Institut Français de Maurice amongst others.

The Data Protection Office has also been actively engaged in many prestigious international meetings with the preparation of elaborate presentations and briefs to showcase the Mauritius data protection journey and experience. The participation of the Commissioner has been deeply appreciated by foreign counterparts.

In addition, the office continued offering free training courses on the Data Protection Act 2017 to interested organisations through the in-house training initiative which was introduced in 2018.

MEXICO

Information regarding the major developments in the data protection field in Mexico since November 2020, provided by Instituto Nacional de Transparencia, Acceso a la Información y protección de datos personales (INAI).

- Code of good practices to guide the online processing of personal data of girls, boys and adolescents. The Code contains a set of fifteen rules that are intended to protect minors so that they can explore, learn and play online, guaranteeing adequate protection of their personal data.

Available at: [codigobuenaspracticasnna.pdf](https://www.inai.org.mx/codigobuenaspracticasnna.pdf) (inai.org.mx)

- Microsite "Secure Personal Data. COVID-19". Created by the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) to provide clear and precise information to holders about the right to protection of their personal data that, where appropriate, will be processed in public institutions or private in order to provide them with the diagnosis, care and follow-up on COVID-19. As well as providing recommendations for those responsible and those in charge of the Public and Private Sector, on the adequate treatment of personal data that they must carry out in the various activities required for the attention of COVID-19 cases, in order to comply with the principles, duties and obligations that the legal framework regarding the protection of personal data establishes.

Available at: [COVID-19 and the processing of personal data](https://www.inai.org.mx/covid-19) (inai.org.mx).

MOLDOVA

Regarding the request to present the main developments in the data protection field since November 2020, the National Center for Personal Data Protection of the Republic of Moldova communicates the following:

Even if the concerned period was one full of challenges, due to the global pandemic situation, the Data Protection Authority of the Republic of Moldova tried to continue its work on the issue of data protection, informing the general public about the rights and obligations regarding data protection, confidentiality and protection of personal data. In order to achieve this goal, the employees of the Center participated in working meetings with public and private authorities. It should be noted that due to the global pandemic situation, 2020 was a limited year in terms of meetings and appointments in the format they used previously to take place. However, some progress has been made.

Legislative developments

We would like to mention about the amendments made by Law no. 124 of July 9, 2020 (in force since August 24, 2020) on the provisions of art. 27 of the Law on personal data protection, which have an important role for the activity related to the control of the legality of personal data processing. The amendments brought essential conceptual and procedural improvements, on the one hand providing clarity to the actions needed to be taken by data subjects filing complaints against the Center as well as by data controllers, and on the other hand establishing expressly organizational aspects such as: procedures, deadlines, criteria and even competencies, which have come to streamline and optimize the institutional capacities related to the control of the legality of the processing of personal data.

On the legislative developments, we also mention that *the Draft Law on Personal Data Protection and the Draft Law on the National Center for Personal Data Protection* were examined in May in the National Security, Defense and Public Order Commission of the Parliament of the Republic of Moldova, in order to be promoted for the second reading.

At the same time, we mention that the Personal Data Protection Authority has continued to develop the segment of information, communication and awareness by proactively providing information and public awareness on the principles of personal data protection. Thus, the Center ensured a continuity of the trainings organized for the civil servants from the central and local public administration.

International cooperation

The establishment and development of international cooperation in the field of personal data protection continued to be one of the key elements in strengthening the functional capacities of the Center in the period concerned.

During the reference period, the Center tried to focus its activity on strengthening bilateral and multilateral relations with external partners both within international organizations and individually.

In order to achieve this goal, Center's employee participated in the working meetings of the European and International Committees. Although the period of reference was a limited one, however the Centre's representatives participated in various conferences, meetings and working groups at international level, such as the plenary meetings of the European Data Protection Board, the plenary meetings of the Council of Europe, and other meetings.

We mention that the Center applied and obtained in the reference period the support from the TAIEX Project in organizing the workshop ***"Processing and protection of personal data in the field of public health in the context of possible global challenges! (COVID pandemic - 19)"***.

The aim of the workshop was to strengthen and enhance the skills of public health representatives on possible challenges that may arise globally (in the context of the pandemic COVID - 19), while respecting the fundamental rights and freedoms of individuals on personal data protection when the processing is necessary for reasons of public interest in the area of public health as well as the adoption of good practices based on relevant case law; setting a balance between the processing, storage, and disclosure of health data and the right to privacy; promoting clarity and specialized analysis, oriented towards the provisions of the law on data protection in the specific field of application - that of health; familiarization of medical representatives with the new challenges related to the processing of personal data etc.

The event was organized for representatives of the Ministry of Health, Labor and Social Protection as well as medical institutions, the Ministry of Justice, the Ministry of Internal Affairs and the General Inspectorate of Police. Personal data protection experts from Croatia, Slovakia and representatives of the Center, had presentations during the event. Based on the global situation of the SARS-COV - 2 pandemic, the event took place online at the end of January 2021 for approximately 300 people, from three different regions: Central, North and South.

Also, on July 7, with the support of the TAIEX project, a conference entitled "*The impact of new technologies, caused by the COVID - 19 pandemic, on the protection of personal data in the public sector*" will be organized.

The aim of the conference is to present the aspects of the impact of technologies on the field of data protection. The event will serve as an opportunity for an exchange of experience and best practices on raising awareness and informing the public sector about cybersecurity, the impact of new technologies caused by the COVID-19 pandemic on personal data protection, and will give the opportunity to examine the benefits that intelligence can bring to state institutions.

NORTH MACEDONIA / MACÉDOINE DU NORD

North Macedonia has formally started the process for ratification of the Protocol 223. Namely, we have drafted the Law on ratification of the Protocol 223, and currently is being reviewed by the Government's bodies. Hence, it is expected for this law to be adopted by the Parliament in die time.

MONTENEGRO / MONTÉNÉGRO

Agency for Personal Data Protection and Free Access to Information

Celebrating January 28th – Personal Data Protection Day – On the occasion of January 28th, and in accordance with the situation caused by COVID pandemic, attention has been drawn through media to the responsibility primarily of individuals to protect their personal data by giving data only where there is a legal basis or to exercise their rights, and also of institutions and organizations to act upon them in a legally prescribed manner, and in accordance with positive practices of best protections.

Cooperation with OECD - OECD is a unique forum on which states operate together to address economic, social and environmental challenges of globalization. Ministry of Public Administration coordinated the preparation of the publication "Competitiveness in Southeast Europe for 2021". Following the submission of this publication and additional clarifications, a meeting was held on December 17th at which the publication was presented and a dialogue was held on the Preliminary Competitiveness Program 2021 (findings, assessments and recommendations for Montenegro).

During the time from November 2020 to June 2021:

- total of **23** consents were issued for introduction of personal data collections i.e. for introduction of video surveillance;
- the Council of the Agency determined **6** opinions regarding the application of the Law on Personal Data Protection;
- **49** letters were sent in which the Agency, interpreting the provisions of the Law on Personal Data Protection, was in function of cooperation with data controllers.
- **1** request for initiating misdemeanor proceedings was submitted to the competent misdemeanor court.

Review of performed inspections:

| November 2020 – June 2021 | | |
|----------------------------------|--------------------------------------|---|
| Total number of inspections - 49 | | |
| Regular inspection | extraordinary inspection | |
| 5 | 39 | |
| Additional inspection | Request for the protection of rights | Initiative for the protection of rights |
| 0 | | |
| Procedure check | 10 | 29 |
| 5 | | |

MONACO

Développements majeurs intervenus en matière de protection des données personnelles

novembre 2020 / juin 2021

ooo

LOI

- Loi n° 1.503 du 23 décembre 2020 renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption (*le registre des bénéficiaires effectifs, le registre des trusts ainsi que le registre des comptes de paiement, des comptes bancaires et des coffres forts, emportant la mise en œuvre, par l'Etat, de traitements d'informations nominatives*)

ORDONNANCES SOUVERAINES et ARRETES MINISTERIELS

Données de santé

- Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé ;
- Arrêté Ministériel n° 2020-764 du 5 novembre 2020 portant application de l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé.

Il définit les conditions de délivrance de la qualification d'hébergeur de données de santé à caractère personnel.

Du secret des correspondances

- Ordonnance Souveraine n°8.010 du 12 mars 2020 portant application de l'article 28-9 de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée

Le Gouvernement entend renforcer le cadre applicable aux secrets des correspondances émises, transmises ou reçues sur des réseaux de communications électroniques en instaurant un régime d'autorisation préalable permettant au Ministre d'Etat de s'assurer du caractère justifié de l'acquisition, la détention, la fabrication, l'importation, l'exposition, l'offre, la location ou la vente de tout appareil ou dispositif matériel comme logiciel de nature à permettre l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de ces correspondances

- Arrêté Ministériel n° 2021-220 du 18 mars 2021 portant application de l'article 28-9 de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, définissant la liste des appareils ou dispositifs matériels et logiciels soumis à autorisation du Ministre d'État

Il définit, dans son annexe, la liste des appareils ou dispositifs matériels et logiciels soumis à autorisation mentionnée à l'article 28-9 de la loi n°1.383 du 2 août 2011, modifiée.

De la transposition du règlement européen eIDAS

- Arrêté Ministériel n° 2020-892 du 18 décembre 2020 portant application de l'article 8 de l'arrêté ministériel n° 2020-461 du 6 juillet 2020

Il définit les critères de reconnaissance des organismes d'évaluation de la conformité des prestataires de service de confiance

- Arrêté Ministériel n° 2020-893 du 18 décembre 2020 portant application de l'article 12 de l'arrêté ministériel n° 2020-461 du 6 juillet 2020

Il définit les critères d'évaluation de la conformité des prestataires de services de confiance qualifiés

- Arrêté Ministériel n° 2020-894 du 18 décembre 2020 portant application des articles 20, 29 et 34 de l'arrêté ministériel n° 2020-461 du 6 juillet 2020

Il définit les critères d'évaluation de la conformité des services de création de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site Internet

- Arrêté Ministériel n° 2021-151 du 18 février 2021 portant application des articles 32 et 33 de l'arrêté ministériel n° 2020-461 du 6 juillet 2020

Il définit les critères d'évaluation de la conformité des services d'horodatage électronique qualifiés.

De l'extension des services de confiance

- Arrêté Ministériel n° 2021-247 du 25 mars 2021 portant application des articles 2 et 3 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance.

Il définit les exigences qui doivent être respectées par les services de confiance d'archivage électronique et de numérisation pour la réalisation d'une copie fiable d'un document dans des conditions qui assurent des garanties fiables quant à la conformité à l'original de la copie ainsi créée

De l'Agence Monégasque de sécurité numérique

- Ordonnance Souveraine n° 8.504 du 18 février 2021 portant application de l'article 24 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique

Elle définit le rôle et les missions de l'Agence Monégasque de Sécurité Numérique en application de la loi n°1.435.

Secteur économique et financier

- Ordonnance Souveraine n° 8.258 du 18 septembre 2020 portant application de la loi n° 1.491 du 23 juin 2020 relative aux offres de jetons, modifiée par l'Ordonnance Souveraine n° 8.467 du 21 janvier 2021
-
- Ordonnance Souveraine n° 8.634 du 29 avril 2021 portant modification de l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la loi n° 1.362 du 3 août 2009, modifiée, relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée
- Ordonnance Souveraine n° 8.635 du 29 avril 2021 portant application de la loi n° 214 du 27 février 1936 portant révision de la loi n° 207 du 12 juillet 1935 sur les trusts, modifiée
- Ordonnance souveraine n° 8.664 du 26 mai 2021 relative aux procédures de gel des fonds et des ressources économiques en application de sanctions économiques internationales
- Arrêté ministériel n° 2019-1088 du 20 décembre 2019 relatif au bulletin de paye électronique

DECISIONS MINISTERIELLES

- Décision du Ministre d'Etat du 4 juin 2021 prise en application de l'Ordonnance Souveraine n° 8.664 du 26 mai 2021 relative aux procédures de gel des fonds et des ressources économiques en application de sanctions économiques internationales
- Décisions du Ministre d'Etat adoptées dans le cadre de la lutte contre la COVID-19

PROJET DE LOI

Projet de loi déposé sur le bureau du Conseil National :

- Projet de loi n° 995 relative à la technologie Blockchain

Un avant-projet de loi, issu de la proposition de loi n° 246, est en cours d'élaboration sur l'utilisation d'un dispositif d'enregistrement numérique sur un registre partagé pour les titres de sociétés non cotées.

AUTORITE DE CONTROLE COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES C.C.I.N

- Examen du projet de loi relative à la protection des données personnelles en cours d'élaboration par les services du Gouvernement

PORTUGAL

Common regime on the protection of personal data applicable in Portugal

Law No 58/2019, of 8 August, which ensures the implementation, in the national legal order, of 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.

<https://dre.pt/pesquisa/-/search/123815982/details/maximized>

Deliberation 2019/494 of the Portuguese Data Protection Authority, which removes certain articles of Law 58/2019.

<https://www.cnpd.pt/decisooes/historico-de-decisooes/?year=2019&type=&ent=>

Regulation No 310/2020 of the Portuguese Data Protection Authority, fixing the value of the fees for the assessment and decision of applications made to the Portuguese Data Protection Authority.

<https://dre.pt/home/-/dre/130887195/details/maximized>

Law No 59/2019 of 8 August adopting rules on the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

<https://dre.pt/home/-/dre/123815983/details/maximized>

SAN MARINO / SAINT-MARIN

On 21 December 2018 the “Consiglio Grande e Generale”, which is the Parliament of the Republic of San Marino, promulgated the Law no. 171 of 21 December 2018 on the protection of individuals with regard to the processing of personal data. The Law no. 171/2018 provides for the establishment of the Data Protection Authority named “Garante per la protezione dei dati personali” which is an independent public authority.

The Law no. 171/2018 is a GDPR-oriented law, i.e. very close to the content of the European Regulation 2016/679 (GDPR).

The Law mentioned above 171/2018 came into force on 5 January 2019.

Article 52 of the Law as mentioned earlier established the Guarantor Authority for the protection of personal data, a collegial body composed of the Collegiate body and the Office, which is responsible for monitoring the application of the Law to protect the fundamental rights and freedoms of individuals with regard to the processing of personal data.

In January and in March 2019 the Consiglio Grande e Generale (the Parliament) appointed the three members of the Collegiate body, and precisely the President, the Vice President and the member.

The Office of the San Marino Data Protection Authority took office on 1 February 2019 and the Board of Auditors on 2 April 2019.

It is the first Data Protection Authority in the Republic of San Marino.

Once established, the Authority began to carry out its tasks and exercise its powers as provided for by Law no. 171/2018.

The Data Protection Authority participated as Observer at the Spring Conference 2019 held in May 2019 in Tbilisi (Georgia), applying to become a member.

In October 2019 the San Marino DPA was accredited as a full member at the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC) now Global Privacy Assembly (GPA).

The Republic of San Marino is a member of the Council of Europe and participates in meetings on data protection, reporting the activities to the Authority for the protection of personal data.

The San Marino DPA, among other activities, organises meetings and training courses. On 28 January of each year, the San Marino DPA celebrates the Data Protection Day organising an event to discuss the main topics related to the data protection and privacy issues. The first Data Protection Day was celebrated on 31 January 2019 by organising an event.

The San Marino Data Protection Authority, in cooperation with the Council of Europe, organised the “Data Protection and Privacy Rights” course within the HELP Programmes. The “launch event” of the course held on 9 October 2020.

SERBIA/ SERBIE

Commissioner for Information of Public Importance and personal data protection

The Report on Developments in the Field of Data Protection

November 2020 – June 2021

I. Legal Framework

Since the adoption of the new Law on Personal Data Protection ("Official Gazette of RS", no. 87/2018), Commissioner and the Government have adopted all bylaws within the defined deadline. The obligation under Article 100 of the LPDP, which stipulates that the provisions of other laws, that refer to the processing of personal data, shall be harmonised with the provisions of LPDP by the end of 2020, has not been fulfilled.

II. Statistical overview of the Commissioner's activities related to personal data protection

| | |
|---|--|
| <u>Supervision over LPDP enforcement:</u> | In the period from 1 November 2020 until 31 May Commissioner completed 96 supervisions |
| Inspection powers | Based on Art. 77-79 of the new LPDP, the Commissioner performs inspection supervision over the enforcement of this Law. The Commissioner has compiled and published the following checklists on his website: <ul style="list-style-type: none">• a checklist for controllers being public authorities• a checklist for controllers other than public authorities In the reporting period 352 checklists were processed. |
| <u>Acting on petitions</u> | Commissioner acted on 122 petitions submitted in accordance with the new LPDP |
| <u>Data transfer</u> | One request for data transfer was submitted to the Commissioner |
| <u>Opinions on laws and other regulations and general acts:</u> | Commissioner issued 39 opinions, of which 25 were opinions on drafts and proposals of laws and 14 were the opinions on other regulations and general acts |
| <u>Initiatives and motions</u> | the Commissioner submitted 50 initiatives and motions to the competent state authorities |

III. Activities of the Commissioner related to the promotion of the right to protection of personal data

National assembly debated Commissioner's Report for 2019 and adopted the conclusions on plenary session on 29th December 2020.

Commissioner submitted Report on Work of The Commissioner for Information of Public Importance and Personal Data Protection For 2020 to the National Assembly on 22 March 2021.

National assembly elected Sanja Unkovic as Deputy Commissioner for information of Public Importance and Personal Data Protection – for Data Protection.

In the period from 19 to 29 April 2021, 22 students of the seventh generation of students of the Faculty of Law, University of Belgrade, attended the professional internship with the Commissioner. During the two-week internship, which was held in the form of a webinar due to the epidemiological situation, students had the opportunity to get acquainted with the work of the Commissioner, his competencies, regulations and practice, in the areas of free access to information of public importance and personal data protection.

Based on the agreement between the Commissioner for Information of Public Importance and Personal Data Protection and the Faculty of Security of the University of Belgrade, 55 students of the first generation completed a short study program "Training of managers for personal data protection".

Commissioner marked the Data Protection Day on 28. January 2021. Due to the pandemic caused by the SARS-CoV-2 virus, only speakers and representatives of a number of the highest state institutions were present, while other interested parties could follow the event live via the official YouTube channel of the Commissioner.

IV. Cooperation with state bodies, civil society organizations and business associations

During the reporting period, the Commissioner cooperated with state bodies, civil society organizations and business associations, as well as other institutions, participating in numerous events, conferences, round tables and meetings that were mostly organized online due to the implementation of measures to combat the COVID-19 pandemic.

V. International and regional cooperation

During this period, the Commissioner continued to have successful cooperation with international organizations and forums (Council of Europe, and Global Privacy Assembly (GPA), as well as with representations of international or transnational organizations in Serbia (UNDP, OSCE, Delegation of the European Union to Serbia, Office Council of Europe in Belgrade, USAID Government Accountability Initiative Project). In the field of personal data protection, the Commissioner participated in meetings with Eurojust, representatives of the European Parliament, the European Data Protection Board (EDPB), the International Working Group on Data Protection in Technology (IWGDPT), the Bureau of the Convention Committee 108, as well as the Global Privacy Assembly (GPA).

VI. Cooperation with the media

From November 2020 the Commissioner achieved cooperation with the media with undiminished intensity. Increased activity was noted during the organization of the Data Protection Day on January 28, 2021. During the reporting period, the Commissioner issued 39 press releases.

VII. COVID-19 pandemic – Commissioner's activities during the pandemic

Since the beginning of the COVID-19 pandemic, Commissioner paid special attention to data protection of infected persons. Thus, even before the beginning of the declared state of emergency, he issued a statement warning the media not to publish personal data of persons suffering from coronavirus, and during the state of emergency he issued an appeal regarding the protection of student health data and a statement on personal data processing during a state of emergency.

SLOVAK REPUBLIC / RÉPUBLIQUE SLOVAQUE

The Office for Personal Data Protection of the Slovak Republic has organised *The Data Protection Day 2021* in form of written articles which were made public and available on our official website. The articles tackled various topics: *Data breach notifications*, *data protection in the context of social media*, *Data protection inspections- examples from practice* and *Frequently asked questions about European Data Protection Board*.

We are also included in ongoing debates on *Protection of Children in Online Environment*, *Special Working Group for Artificial Intelligence*, *Working Group for Smart Mobility*, *Working Group for Standardization Operating under the authority of the Ministry of Investments, Regional Development and Informatization of the Slovak Republic*. As members of these working groups, we are in the position of data protection watchdog.

We are member of *Association of Cybersecurity (Slovakia)* and *Committee of the Government of the Slovak Republic for the Digitization of Public Administration and the Digital Single Market at Ministry of Investments, Regional Development and Informatization of the Slovak Republic*.

As far as international cooperation is concerned, we are active member of *European Data Protection Board*, *Council of Europe T-PD group*, *General Privacy Assembly*.

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- person & on-line).

Beside above mentioned activities, we support our employees in self- education, we organise internal seminars in our Office with data protection topics as well as soft skills mostly used in their professional life.

SLOVENIA / SLOVENIE

Report by the Information Commissioner

(2020, 2021)

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 and the Information Commissioner Act.

The work of the IC in the field of personal data protection in the last part of 2020 and the first half of 2021 was marked by an epidemic that showed all over the world how fragile the balance between fundamental human rights is. The biggest challenges in this period were also related to the fact that Slovenia has still not adopted rules for the implementation of the GDPR. However, draft of new Personal Data Protection Act has been prepared and published on 13th May 2021 by the competent Ministry and submitted for expert consultation. The timing of the adoption of the new Personal Data Protection Act is very difficult to envisage at the time. In November 2020, the Law on the protection of personal data in the field of criminal proceedings (i. e. ZVOPOKD) was finally adopted.

The trend of increasing numbers of inspection procedures and appeal procedures regarding the exercise of data subjects' rights continued in 2020 and still continues in 2021. In 2020, the IC noted a significant increase in the number of petitions (1,018 inspection initiatives received) and complaints regarding the data subjects' right to access personal data concerning him or her (226 complaints received). At the international level, the IC conducted 200 cross-border cooperation procedures, and also received 120 notifications of personal data breaches and 5 notifications of violations of patient data under the Patients' Rights Act. Both, complaints and offences mainly concerned, similar as in previous years, unlawful processing of personal data, unlawful video surveillance, unlawful direct marketing and unlawful access to personal data files. In practice, irregularities are still largely result of ignorance of the law.

The IC noted that the majority of controllers and processors want to act in accordance with the law, for which clear regulations and an understandable definition of the obligations are a prerequisite. This proved to be critical during the epidemic, especially in the areas of employment and education. The IC noticed a worrying trend of unsystematic regulation of some serious interferences with privacy and attempts to reduce the already achieved level of personal data protection. Serious problems, as well as individual violations, were caused by vague, unclear or absent instructions, which made it impossible to implement certain measures related to the epidemic in practice. The IC therefore paid a lot of attention to compliance and prevention and in 2020 advised a total of 3,183 individuals and legal entities (issued 1,331 written opinions and advised 1,852 times by telephone), and devoted a special subpage on the website to the publication of opinions and recommendations related to protection of personal during the epidemic. In 2020, the IC also issued 85 opinions on proposed amendments to the regulations.

Regardless of the special circumstances, the IC conducted 34 free lectures in 2020, most of them using online tools. It has also successfully implemented the iDECIDE project, funded by the European Union, aimed at raising awareness of three target populations: minors, the elderly population and the working population. The IC also paid special attention to the data protection officers. The data protection officer has already been appointed by more than 2,300 controllers and processors, and several hundred of them have not yet fulfilled this obligation. Among the most important achievements in 2020, it should be emphasized that Slovenia, as the second country, has successfully prepared standard contractual clauses for the regulation of contractual processing of personal data in accordance with Article 28 of the GDPR.

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).

In the week of the 3rd anniversary of the GDPR the IC hosted an online meeting of the "Initiative 20i7", in which the IC and senior representatives of supervisory authorities for personal data protection from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Kosovo and Macedonia every year exchange experiences and address challenges in the field of protection of privacy. This year, special attention was paid to personal data protection solutions in epidemic-related measures.

SWEDEN / SUÈDE

Swedish Authority for Privacy Protection

As of 1 January 2021, the Swedish Data Protection Authority has a new name, Integritetsskyddsmyndigheten (IMY) or the Swedish Authority for Privacy Protection in English.

In October 2020, the IMY published a report regarding complaints from data subjects according to the GDPR. The report showed that many complaints relate to questions of security for personal data but the major part relate to data subjects' rights such as the right to deletion and right of access to personal data. Following this report, the IMY initiated a project of investigating complaints regarding data subjects' rights in November 2020. The work plan for 2021-2022 also puts an increased focus on investigations based on complaints from individuals, both in order to enforce data subjects' rights and as an effect of the cooperation between EU/EEA data protection authorities.

The IMY has concluded several other investigations encompassing the private sector, the health care sector and law enforcement authorities. In 2020, IMY issued administrative sanctions of, in total, 150 million SEK. The IMY also received 4 600 data breach notifications, 3 200 complaints from individuals and almost 14 000 questions by phone and in writing. These, and other, statistics have been published in IMY's annual report of 2020:

<https://www.imy.se/publikationer/arsredovisning-2020/>

Other publications from IMY include a specific privacy report (Nationell integritetsrapport) which describes the current situation in terms of privacy and new technology and provides recommendations on what the key factors should be in the privacy policy area. This report was published in January 2021 as a first result of a task to the IMY from the Government to, every fourth year, follow and report on the major developments regarding privacy protection in Sweden.

<https://www.imy.se/publikationer/integritetsskyddsrapport-2020/>

In May 2021, IMY issued new guidance on video surveillance and this was followed by holding a virtual training session on video surveillance issues. IMY will also hold virtual training sessions on the GDPR rules in May/June 2021.

In 2020, the IMY gave opinions on legislative proposals in 137 cases, an increase compared to previous years. Some of these proposals were related to the Covid-19 pandemic but they also range from issues regarding whistle blowing, direct access for law enforcement authorities to new technology in the health and welfare sector.

IMY has also continued to cooperate actively with other data protection authorities in the EU/EEA, both within the EDPB and in individual cases that involve cross border processing.

In May 2021, IMY launched a new website: www.imy.se where more information on IMY and its activities can be found.

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

Signature de la Convention 108+

Conformément aux règles nationales de procédure législative, l'assemblée nationale a approuvé le protocole d'amendement en juin 2020. La date de ratification de cet accord n'est en revanche pas encore connue mais est estimée au 2^e semestre 2022, voire au 1^{er} semestre 2023. La Suisse ratifiera le Protocole dès que les mesures prévues dans le cadre de la nouvelle loi et destinées à mettre en œuvre la Convention seront entrées en vigueur (cf. ci-après), conformément à l'art. 6 par. 2 du protocole d'amendement.

Adoption de la révision totale de la loi fédérale sur la protection des données

L'assemblée fédérale a adopté le 25 septembre 2020 la nouvelle loi sur la protection des données (LPD). Le délai référendaire a expiré le 14 janvier 2021 sans avoir été utilisé. La nouvelle loi fédérale sur la protection des données doit encore être mise en œuvre et nécessite l'adoption de nombreuses ordonnances pertinentes. Son entrée en vigueur, prévue au plus tôt pour le 2^e semestre 2022, coïncidera avec le dépôt de l'instrument de ratification de la convention 108+ (cf. ci-dessus ainsi que le projet de loi publié dans la Feuille fédérale, FF 2020 7397 : <https://www.admin.ch/opc/fr/federal-gazette/2020/7397.pdf>).

Décision d'adéquation de la législation suisse toujours attendue

La Suisse fait partie des pays dont la Commission européenne est en train de réexaminer ses décisions d'adéquation en vertu de l'art. 97 du règlement (UE) 2016/679. La procédure a subi des retards en raison de la pandémie 2019. Le projet de décision est attendu en juin / juillet 2021.

Certificat sanitaire

La base juridique pour le certificat sanitaire ayant été adoptée par le Parlement à la mi-mars 2021 (cf. art. 6a de la Loi fédérale sur les bases légales des ordonnances du Conseil fédéral visant à surmonter l'épidémie de COVID-19 [Loi COVID-19 ; RS 818.12] : <https://www.fedlex.admin.ch/eli/cc/2020/711/fr>), le PFPDT accompagne les travaux relatifs au certificat national COVID pour les personnes vaccinées, testées et guéries. La compatibilité du certificat sanitaire suisse avec le « certificat vert numérique » de l'UE est un aspect essentiel. Les exigences du PFPDT concordent, pour l'essentiel, avec l'avis conjoint du Comité européen de la protection des données et du Contrôleur européen de la protection des données concernant la proposition de règlement relatif au « certificat vert numérique » de l'UE (cf. actualité du 13.04.21 « Certificat de vaccination contre le COVID-19 » ; https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news.html#1445828519).

Les travaux au niveau suisse ont également examiné un éventuel usage du certificat sanitaire à d'autres situations, telles que l'accès à des restaurants ou à des manifestations sportives, afin d'assouplir les restrictions actuellement en vigueur. Le PFPDT a exigé que toute utilisation ultérieure du certificat sanitaire soit conforme aux exigences légales de protection des données, notamment aux principes de proportionnalité et de minimisation des données. Le PFPDT a proposé l'introduction d'un deuxième code QR pour l'utilisation ultérieure du certificat sanitaire, contenant moins de données. En effet, si la vérification de l'identité ainsi que l'existence de l'immunité des personnes peuvent être exigées pour l'accès à certains lieux, l'exigence de divulgation d'autres informations, telle que la raison de l'immunité, ne saurait être admise.

Réseaux sociaux victimes de fuite de données

Suite aux fuites massives de données personnelles survenu entre autre auprès de Facebook et de LinkedIn, le PFPDT a publié sur son site internet des mesures générales pouvant aider d'une part à déterminer si une personne est concernée et d'autre part à se protéger. Il a entre autre conseiller de suivre les instructions des entreprises concernées ainsi que de changer de mot de passe. Le PFPDT a également pris contact avec ses homologues étrangers européens et continue à suivre l'évolution (cf. actualité du 13.04.21 « Réseaux sociaux victimes de fuites de données » ; https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news.html#-1784241451).

TURKEY / TURQUIE

Data Protection Authority

Turkish Personal Data Protection Authority (Authority) continue to increase its capacity since its foundation in 2017. In order to increase its qualified human resources capacity, the Authority has recruited junior personal data protection experts in January 2021. Along with capacity increasing, the effectiveness of the Authority both at national and international level is gradually increasing. In addition, in Action Plan of Human Rights - published in April 2021 by the Ministry of Justice - it is declared that the effectiveness of the Personal Data Protection Authority will be improved under the goal of improving the effectiveness of human rights institutions.

Legal Framework

Personal Data Protection Board of the Authority (Board) takes Decisions and Resolutions as a result of examination of complaints, notices and personal data breach notifications. The summaries of new Board Decisions are published on Authority's official website. Recently, by the Resolution of the Personal Data Protection Board dated 22/12/2020 and numbered 2020/966, it is decided that in order to prevent sending documents that includes personal data of third parties in a way that violates the Personal Data Protection Law, in accordance with paragraph (1) of Article 12 of the Law, data controllers shall take necessary administrative and technical measures in order to establish mechanisms to verify the accuracy of the contact information of data subjects.

Besides, many working groups follow the latest developments and carry out studies on personal data protection in different fields and sectors. Also a working group continues its work in order to provide legislative alignment between the Personal Data Protection Law No. 6698 and General Data Protection Regulation (GDPR) and those working groups continue their work.

Complaints, Personal Data Breach Notifications and Administrative Fines

There has been a rapid increase in complaints, notices and personal data breach notifications made to the Authority over the years. The number of complaints and notices Authority received is 59 in 2017, 310 in 2018, 1120 in 2019, 2297 in 2020 and 1185 as of May 2021. 3251 of these complaints and notices were concluded. In addition, 4223 of 4373 complaints received by our citizens living abroad were concluded. The number of personal data breach notifications reported to the Authority is 1 in 2017, 28 in 2018, 139 in 2019, 228 in 2020, 150 as of May 2021. 334 of these notifications were concluded. In order to prevent possible adverse outcomes for the data subjects, 95 of them was published on the Authority's website in accordance with Board Decision.

As of May, the Board has decided to impose administrative fine of 45.070.828 TL on data controllers due to unlawful practices. About 9.580.000 TL of these figures are fines imposed this year and 21.390.000 TL in 2020.

Transfer of Personal Data Abroad

The applications of commitment made by data controllers with regard to the transfer of personal data abroad continue to be evaluated within the scope of Article 9(2) of the Personal Data Protection Law No 6698 in order to grant permission for the data transfer by the Authority.

International Activities

Authority has actively participated to the online meetings, exchanged information and made contribution to various documents particularly about personal data protection in digital economy organized by international organizations as Council of Europe ETS 108, OECD, G20, GPA, EU since November 2020.

Awareness Raising and Training Activities

Authority organized, co-organized or participated to various online seminars, conferences, panels on personal data protection. Many online training seminars on personal data protection legislation and its enforcement are provided for the staff of public entities, universities and NGOs.

In order to raise awareness on the personal data protection, three contests in the field of article, slogan and caricature is held in March and April 2021.

Publication Activities

Turkish Journal of Privacy and Data Protection - a peer-reviewed, scientific/academic journal where the research and review articles on personal data protection - is published twice a year by the Authority since June 2019. Fourth issue of the Journal has published in December 2020.

A public service announcement and an animation video about the importance of personal data protection published on the Authority's official website since November 2020

UKRAINE

The Ukrainian Parliament Commissioner for Human Rights

INTRODUCTORY SUMMARY

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was ratified by Ukraine in 2010. In June 2010 Ukraine adopted Personal Data Protection Law closely modelled on the Convention 108.

The Ukrainian Parliament Commissioner for Human Rights (the Commissioner) commenced activity as the personal data protection supervisory authority on 1 January 2014. As of May 2021 Department on personal data protection, coordinated by the Representative of the Commissioner for personal data protection, is staffed with 23 positions, including 16 occupied by actually working personnel.

Currently, the Commissioner, as an official entrusted by law with the powers of a personal data protection supervisory authority, meets the criterion of independence. However, certain functions, in particular the imposition of administrative fines, are inconsistent with the nature of the Commissioner's mandate.

ACTIVITIES TO BRING CURRENT LEGISLATION ON PERSONAL DATA PROTECTION IN LINE WITH EUROPEAN STANDARDS

According to the Action Plan for the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other hand, approved by the Cabinet of Ministers of Ukraine dated October 25, 2017 № 1106, it is stipulated to improve current legislation on personal data protection in order to bring it in line with the EU General Data Protection Regulation (hereinafter - Regulation (EU) 2016/679). In view of that, the Ukrainian Parliament Commissioner for human rights has taken a decision on establishing the Interagency Working Group to develop legislative proposals in the field of personal data protection, involving stakeholders, - representatives of state authorities, international organizations, national and international experts in this field.

As a result, a new version of the Law of Ukraine "On Personal Data Protection" (hereinafter - the draft law) was developed, which reflected as much as possible the novelties of the Regulation (EU) 2016/679. Under the Ukrainian legislation the Commissioner is not authorised for legislative initiative, therefore the draft law developed by the Secretariat of the Commissioner was submitted to the Parliamentary Committee on Human Rights, Deoccupation and Reintegration of Temporarily Occupied Territories in Donetsk, Luhansk Regions and the Autonomous Republic of Crimea, City of Sevastopol, National Minorities and Interethnic Relations for consideration by People's Deputies of Ukraine and decision-making on its submitting to the Verkhovna Rada of Ukraine.

Subsequently, a working group set up under the before mentioned Parliamentary Committee with the participation of People's Deputies of Ukraine, representatives of public authorities, experts in this field and representatives of public and international organizations has been working on the draft law.

In early 2021 a new version of the Law "On Personal Data Protection" was presented for public consultations and general discussion of the draft law.

The issue of establishing and operating a new supervisory authority in the field of personal data protection is not currently included in the draft law; however, the working group is considering the development of a draft law that will include the issues of organization of both the supervisory authority in the field of personal data protection and access to public information. It should be noted, that the issue of supervisory

authority creation is beyond the competence of the Commissioner, so it is expected that such a decision will be taken by the Parliament jointly with the Government. At the same time, the Commissioner supports the need to create a separate supervisory authority in the field of personal data protection, if such a decision is made by the Parliament.

EVALUATION OF LEGAL INSTRUMENTS AND DRAFT LAWS TO BE ADOPTED WITH REGARD TO THE CURRENT PERSONAL DATA PROTECTION STANDARDS

The Commissioner regularly provides evaluation and, where relevant, recommendations on adaptation of legislation with regard to the personal data protection standards.

In 2019-2020 a number of violations of the right to privacy by collection companies in the process of financial debt collection were identified by the Commissioner. In order to regulate the activity of collection companies and to guarantee personal data protection the Commissioner together with the National Bank of Ukraine and People's Deputies worked on a relevant draft law.

In early 2021 the developed draft law was adopted and, inter alia, included a general ethical code of conduct of the collection companies in order to provide a sufficient level of personal data protection.

In order to combine legislative regulation and public awareness in March 2021 the Commissioner together with the National Bank of Ukraine and other stakeholders launched the All-Ukrainian information campaign to protect the rights of consumers of financial services "Know your rights".

DATA PROTECTION IMPACT ASSESSMENT OF THE GOVERNMENTAL PROJECTS

The Commissioner has been also providing governmental digital projects, concepts and online platforms such as Diia, Dii Vdoma, E-residency, Concepts for the Development of Artificial Intelligence in Ukraine and for the E-health development, with data protection impact assessment prior to the launch and has been giving her position and recommendations on measures to be taken for the strengthening of personal data protection. This does not preclude further inspections after the implementation of the projects.

RAISING PUBLIC AWARENESS

Raising public awareness in the area of personal data protection as an instrument of violations prevention remains one of the priorities of the Commissioner's activity.

The Commissioner together with the Office of the Council of Europe in Ukraine and the EdEra online education studio created an online course "Personal Data Protection". It consists of two versions: basic one and advanced version for public servants and those who work with personal data. The course has already been launched and is available free-of-charge for everyone.

Therewith, Office of the Commissioner has initiated a translation of the updated Handbook on European data protection law edition, as well as the Guidelines of the Consultative Committee of the Convention 108 on Children's Data Protection in an Education setting into Ukrainian that are made available on the website of the Commissioner to be taken into account by all stakeholders. The translation has been provided by the Council of Europe Office in Ukraine in the framework of a joint project of the European Union and the Council of Europe "European Union and Council of Europe working together to strengthen the Ombudsperson's capacity to protect human rights" (hereinafter-Project).

A compilation of most recent ECHR case-law regarding personal data protection has been also developed by the Office of the Commissioner, translated into Ukrainian with the support of the Project and made available on the official web-site of the Commissioner.

RAISING AWARENESS OF DATA CONTROLLERS AND PROCESSORS

Personal data protection specialists of the Commissioner's Office regularly develop recommendations and short guidelines on selected and most relevant issues. As well as on European standards to be implemented.

In November 2020 two lectures in mixed format were held by the Department on personal data protection for the State Migration Service of Ukraine. In April 2021 five online-lectures on various aspects of personal data protection were held for National Police of Ukraine.

At the same time a tool for business to evaluate the compliance with personal data protection standards was developed as a result of cooperation of the UNDP Ukraine, the Ministry of Digital Transformation, the Commissioner's Office and Ukrainian NGOs. The tool is designed as a test with general recommendations and is aimed at small and medium business.

UNITED KINGDOM – OVERSEAS TERRITORIES / ROYAUME-UNI – TERRITOIRES D'OUTRE-MER GIBRALTAR

Gibraltar Regulatory Authority

The Data Protection Act 2004 (the “DPA”) designates the Gibraltar Regulatory Authority (“GRA”), as Data Protection Commissioner (the “Commissioner”), to be the supervisory authority in Gibraltar. The general functions conferred on the Commissioner in relation to the tasks and powers of the supervisory authority are assigned under Part V and VI of the DPA.

As of the end of the Brexit transition period (i.e., 31st December 2020), the European Union’s General Data Protection Regulation 2016/679 (the “EU GDPR”) no longer has direct effect in Gibraltar. There have however not been any substantive changes to data protection law in Gibraltar as Her Majesty’s Government of Gibraltar have committed to continue to ensure that Gibraltar applies the highest standards of data protection. The EU GDPR has in effect been “transposed” into local law to create the “Gibraltar GDPR” and the data protection regime in Gibraltar therefore remains largely the same as it was prior to Brexit.

The DPA alongside the Gibraltar GDPR, provide a comprehensive and modern framework for data protection in Gibraltar.

The following summarises key developments in Gibraltar’s data protection arrangements from November 2020 to May 2021.

International:

- (a) The GRA is an active participant of the Global Privacy Assembly’s International Enforcement Working Group. The GRA has discussed and engaged with other Data Protection Authorities on several areas of concern / interest in this context and has been actively engaging on key projects such as the joint action on Video Conferencing (“VTC”) Companies - the GRA and several other data protection authorities [published an update](#) in relation to their engagement with VTC service providers, following an open letter in July 2020 where the participating authorities expressed privacy concerns relating to the surge in VTC use. Further engagement with the VTC service providers continues.

Local Engagement:

- (a) The GRA signed an MOU with the Gibraltar Gambling Commissioner, the aim of which is to facilitate co-operation and communication between both regulatory bodies. Under the terms of the MOU, the GRA and the GGC have agreed to the exchange of information as they may consider beneficial in the exercise of their respective regulatory functions. In particular, the MOU is intended to enable both regulators to identify and collaborate on areas of common interest, such as data security.
- (b) On 9th February 2021, the GRA participated in a multi-agency campaign as part of internationally celebrated Safer Internet Day. An awareness-raising audio-visual was created, with this year’s theme being “An internet we trust: Exploring reliability in the online world”.

Regulatory matters:

- (a) **Guidance notes:** The GRA released or updated Guidance Notes on the following topics: Getting ready for a “no-deal” Brexit (update); Concepts of Data Controller and Data Processor; The rights of individuals; The Right of Access (update); Consent (update).

- (b) **Workshops:** As part of their attempts to improve the standards of personal data processing by organisations established in Gibraltar, the GRA carried out a Workshop for Data Protection Officers (“DPOs”) as well as a separate Brexit-focussed workshop for DPOs. The former included sessions on Data Protection Impact Assessments, The role of DPOs, Individuals’ Rights, and Accountability under the Gibraltar GDPR.
- (c) **Awareness:** In addition to the annual school campaign (includes a survey and presentations to students) and ongoing social media campaigns, the GRA launched an eight-week long campaign titled “The Rights of Individuals under the Gibraltar GDPR”. The campaign includes a Guidance Note, a set of infographics and a collection of short videos. These aim to raise awareness of privacy and data protection, and in particular, the rights that individuals have in relation to their personal data.
- (d) **Enforcement:** During the period reported on, the GRA issued a Notice of Intent to issue a penalty, which was followed by a penalty notice.

URUGUAY

Since November 2020, and through Law N° 19.924, of 18th. December 2020, Uruguay has modified article 4 and added an article 18 bis to Law 18.331, of 11th. August 2008, to include in its legislation the concept of Biometric Data and obligations related to such data. In the new provisions, Biometric Data is defined as: "personal data obtained from a specific technical treatment, related to physical, physiological or behavioral characteristics of a natural person who allow or confirm the unique identification of said person such as fingerprint data, image or voice recognition". It has also imposed the obligation of performing a data protection impact assessment prior to the treatment of such data.

In april 16th. 2021, through Law N° 19.948, Uruguay has approved Convention 108+.

