KPMG

Data privacy newsletter

KPMG Global Legal Services

June 2019

Contents

Introduction

Welcome to the KPMG Global Legal Services newsletter on developments in the world of data protection and privacy law. KPMG member firms are proud of their global network, with privacy lawyers, enabling KPMG professionals to offer an international service to clients in this area.

KPMG's global network enables us to bring you various snapshots of recent developments in a selection of the jurisdictions. We live in fast changing times in this area. Our articles seek to demonstrate the state of development of the law in various jurisdictions whilst also showing the very broad impact that data protection law has. In this edition topics include AI, screen scraping, regulatory actions and statistics, new consumer rights, political campaigning, marketing, journalism, surveillance, indebtedness, data breaches, privacy impact assessments, new obligations for employers and transparency in relation the official app of the Spanish soccer league.

Argentina

A. New personal data protection bill

New personal data protection bill

On 18 September 2018, the Argentine Executive Branch submitted to the National Congress a new Personal Data Protection Bill (hereinafter, the "Bill"), which is intended to replace the current regime on personal data protection set forth in Law No. 25,326, enacted in 2000.

The aim of the Bill is to update the current law to the technological advances and legal developments that have occurred in last years, especially regarding the passing of the GDPR.

The most significant changes included in the Bill in relation to the Law N° 25,326 currently in force, are the following:

— The Bill limits the concept of personal data to human persons, abandoning the criterion of the Law N° 25,326 that includes legal entities.

— The Bill introduces tacit consent for the processing of data, provided that it emerges in an express manner from the context of the processing of data and from the conduct of the owner of the data, in order to demonstrate the existence of his/her authorization.

— The registration of data bases shall not be required. This amendment to the current law highlights the principle of proactive responsibility and widens the protection of personal data, not limiting it to the one included in a data base.

— The Bill incorporates the obligation to report security incidents to the enforcement authority as well as to the data owner.

— The Bill introduces the Data Protection Delegate, in certain specific cases.

— The Bill establishes the cases in which international data transfer is considered legal, such as the transfer to any company of the same economic group.

— The Bill incorporates the obligation of the data controller to carry out impact analysis in cases that due to their nature, scope or purposes, it is likely to entail a high risk of affecting the rights of the data subjects.

— The Bill introduces substantial increases in the penalties for infringement. The current maximum fine amounts to AR$100,000 (approximately EUR 2,000). Under the Bill, the maximum fine will be set by reference to 500 times the required minimum wage for individuals (AR$ 6,250,00 – approximately EUR 125,000).

— The Bill shall enter in force in a two-year term as from its publication in the Official Gazette, providing such term as a transition period.

If you have any questions, please let us know

Juan Martin Jovanovich
Partner
KPMG in Argentina
T: +541143165805
E: mjovanovich@kpmg.com.ar

Maria Ximena Perez Dirrocco
Senior Manager
KPMG in Argentina
T: +541143165915
E: mperezdirrocco@kpmg.com.ar

María Amelia Foiguel Borci
Manager
KPMG in Argentina
T: +541148915633
E: mfoiguelborci@kpmg.com.ar

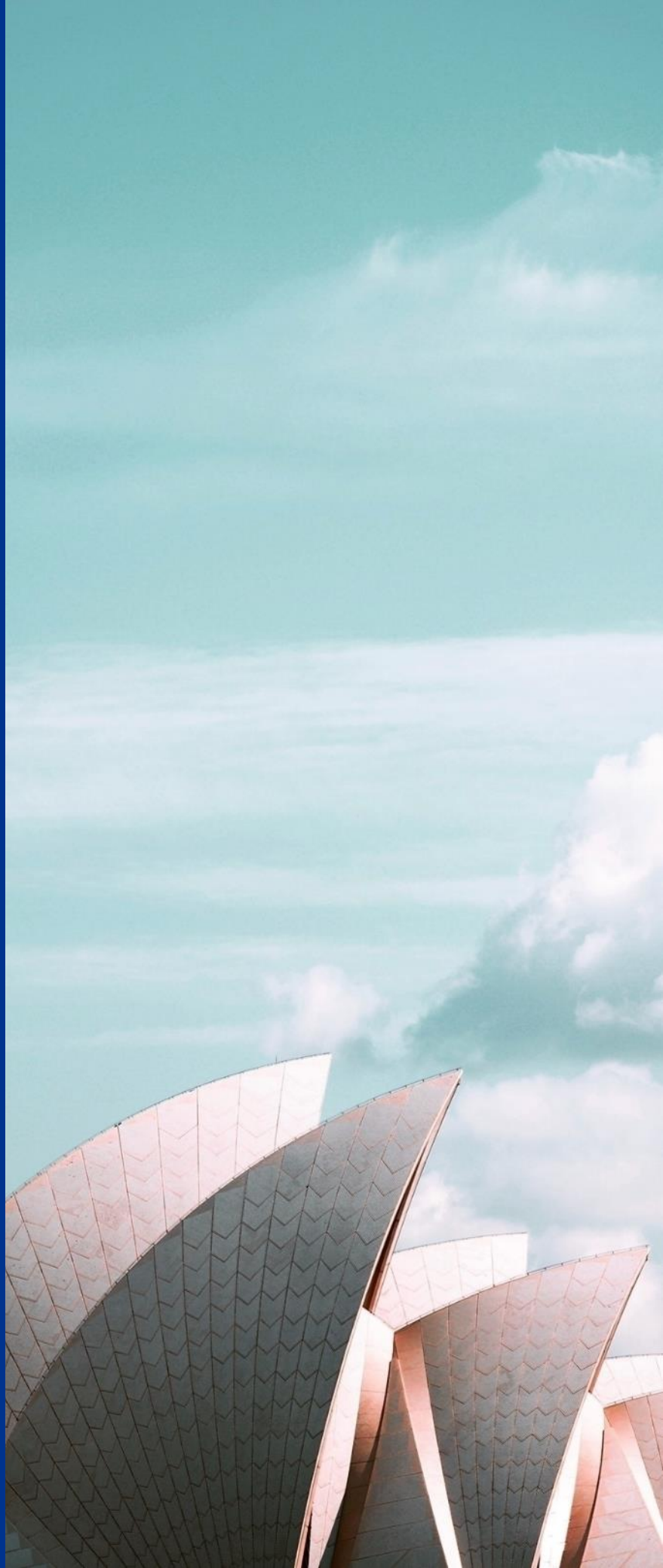
Australia

A. Consumer data rights

B. Public consultation on AI ethics framework

C. Screen scraping

D. The Assistance and Access Act

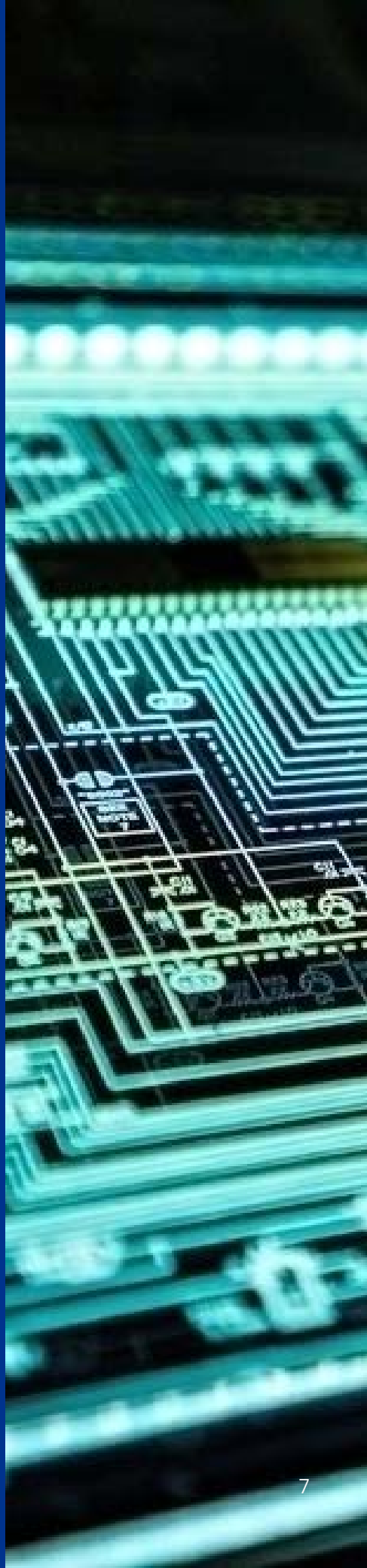


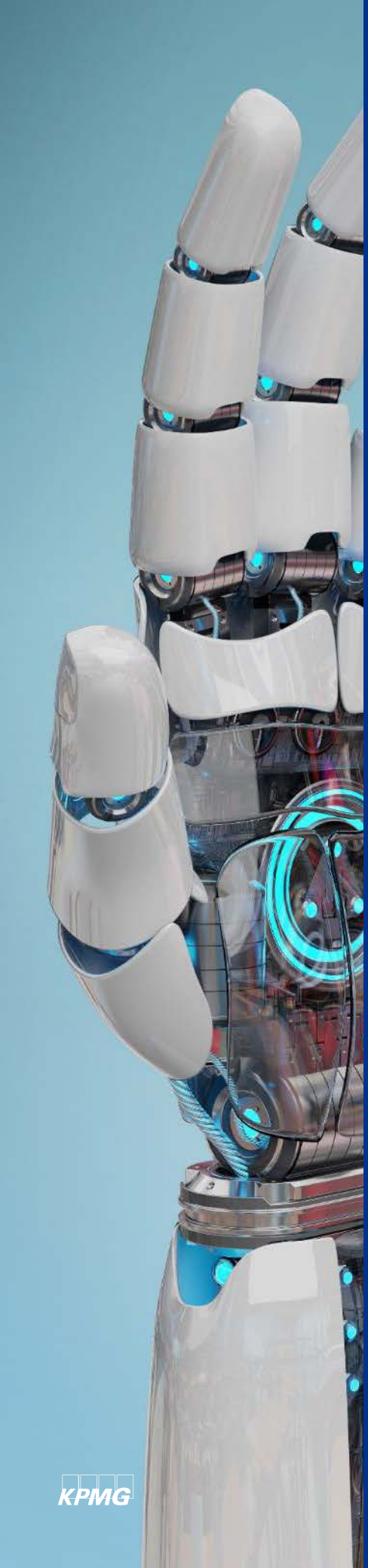
Consumer data rights

The Australian Government is developing a Consumer Data Rights Regime which will be incrementally rolled out across sectors beginning with banking, energy and telecommunications. The aim of the new regime is to provide individuals and business with a right to access specified data about them held by businesses.

The new rules will be regulated by the Australian Competition and Consumer Commission, and supported by the Office of the Australian Information Commissioner and the Data Standards Body.

Working drafts of the Consumer Data Standards are being developed by CSIRO's Data61 with input from a broader Consumer Data Rights Community. The most recent working drafts were released in May 2019.





Public consultation on AI ethics framework

The Australian Government is conducting a consultation process to inform its approach to developing an Ethics Framework for artificial intelligence.

The process commenced mid 2018 with consultative workshops hosted in four capital cities of Australia. These workshops formed the basis for a discussion paper titled 'Artificial Intelligence: Australia's Ethics Framework' which was released in April 2019. This discussion paper sought to facilitate discussion about AI and ethics and called for submissions. The period for making such submissions recently closed.

KPMG Australia made two submissions, one on behalf of KPMG Australia, and the other as members of the Future AI Forum.

Our submissions are available here:

— KPMG Australia Submission

— KPMG Future AI Forum

Screen scraping

Given dramatic increases in the volume and variety of Big Data available on the web, web-scraping and web-crawling technologies present considerable opportunities for commercial entities, researchers and interested individuals to find, collect and make sense of large amounts of information.

There are concerns, however, that individuals may be able to be identified from publicly available non-personal or de-identified data in data-scraping contexts.

These technologies are presenting novel issues in the data privacy landscape and legal consideration to date has been limited. For further exploration of these issues, please see:

— Screen-scraping, de-identification and privacy

— Artificial intelligence (AI) and the great privacy challenge

The Assistance and Access Act

The Assistance and Access Act came into effect late last year and gives intelligence and interception agencies (including ASIO, ASIS and the ASD) the ability to monitor the use of encrypted technologies by terrorists, sex offenders and criminal organisations by enlisting support from a broad range of organisations and through increased computer access and search warrants.

The legislation broadly applies to 'designated communications providers' which can include any individual or entity who provides, or provides a service that facilitates, an electronic service that has one or more end-users in Australia.

The Act gives the Attorney General the ability to issue a Mandatory Technical Capability Notice which can require the provider to undertake any of a list of actions in order to provide assistance.

If you have any questions, please let us know

Kate Marshall
Partner
KPMG Australia
T: +61 3 92885767
E: katemarhsall@kpmg.com.au

Meagan Ryan
Manager
KPMG Australia
T: +61 3 8663 8575
E: mryan6@kpmg.com.au

Jey Jeyabala
Senior Consultant
KPMG Australia
T: +61 3 86638963
E: jjeyabala@kpmg.com.au

Rebecca Breadmore
Consultant
KPMG Australia
T: +61 3 8663 8348
E: rbreadmore@kpmg.com.au

Bulgaria

A. Some new enforceable rules for employers

B. Provisions on media challenged before the constitutional court

Some new enforceable rules for the employers

The amended Bulgarian Personal Data Protection Act (PDPA), adopted in the beginning of this year, gave answers to various questions which had attracted public attention since the adoption of the GDPR, but which had not been previously resolved by means of an enforceable legislative act, especially in the area of employment.

Now, the PDPA explicitly provides that each employer shall determine explicit retention period for CVs and supporting documentation, which cannot be longer than six months.

Another specific rule obliges employers to adopt and inform employees of policies and procedures related to: (a) systems for reporting of violations, such as hotlines; (b) the use of corporate resources, such as internet and email; and (c) systems for supervision over access to premises, working hours and labour discipline in general. These policies aim to reconcile the conflict between employees' right to privacy and the exercise of disciplinary powers.

Provisions on media challenged before the constitutional court

The GDPR provides that Member States should reconcile the freedom of journalistic expression and information with the right to protection of personal data.

The amended Bulgarian PDPA now includes rules on processing personal data for journalistic purposes, including with regard to production of videos and photos at public places and in the course of the performance of public service by an individual.

The PDPA provides a non-exhaustive list of ten criteria to be taken into consideration to assess whether disclosure of personal data in the course of a journalistic survey would be in line with the right to privacy of personal life, such as whether the individual is a public figure, the nature of the personal data themselves, the necessity of the disclosure for the revealing matters of public interest, etc.

These specific criteria for disclosure, which limit journalists, provoked the Head of State to exercise his constitutional powers to challenge the bill and invoke its second vote in Parliament. The veto was eventually overthrown.

Cases of the Supervisory Authority

As a corollary of the public debate, the Bulgarian Commission for Personal Data Protection (CPDP) received complaints and requests for interpretation of the provisions on disclosure of personal data for journalistic purposes. Three of the more notable cases concerned:

— Disclosure of a photo and allegations of criminal activity in a local newspaper

— Publishing information concerning the previous convictions of an individual

— Disclosing wealth details for regular citizens along with details for politicians involved in a corruption scandal.

All of them were resolved by the CPDP, which based its resolutions on the interpretation of the above mentioned criteria for admissibility of disclosure, provided by the PDPA.

Constitutional Court Case

Meanwhile, the Constitutional Court was referred to by 55 members of Parliament (MPs), who challenged the consonance of the PDPA with the provisions of the Constitution.

On the grounds of conflict with the principle for rule of law, the 55 MPs required the PDPA's criteria for disclosure admissibility to be proclaimed non-compliant with the Constitution. Thus, these criteria shall become inapplicable in court and by supervisory authorities.

Until the matter is resolved by the Constitutional Court, any court proceedings, including for appeal against acts of the CPDP, based on the above mentioned criteria will be stayed. Furthermore, the CPDP may need to reshape its principle statements, which relied on the challenged provisions.

If you have any questions, please let us know

Juliana Mateeva
Partner, Legal Advisory
KPMG in Bulgaria
T: +35929697600
E: jmateeva@kpmg.com

Petya Yordanova-Staneva
Manager, Legal Advisory, CIPP/E, CIPM
KPMG in Bulgaria
T: +35929697600
E: psaneva@kpmg.com

Teodor Mihalev
Lawyer
KPMG in Bulgaria
T: +35929697600
E: tmihalev@kpmg.com

Czech Republic

A. Czech act on personal data processing adopted

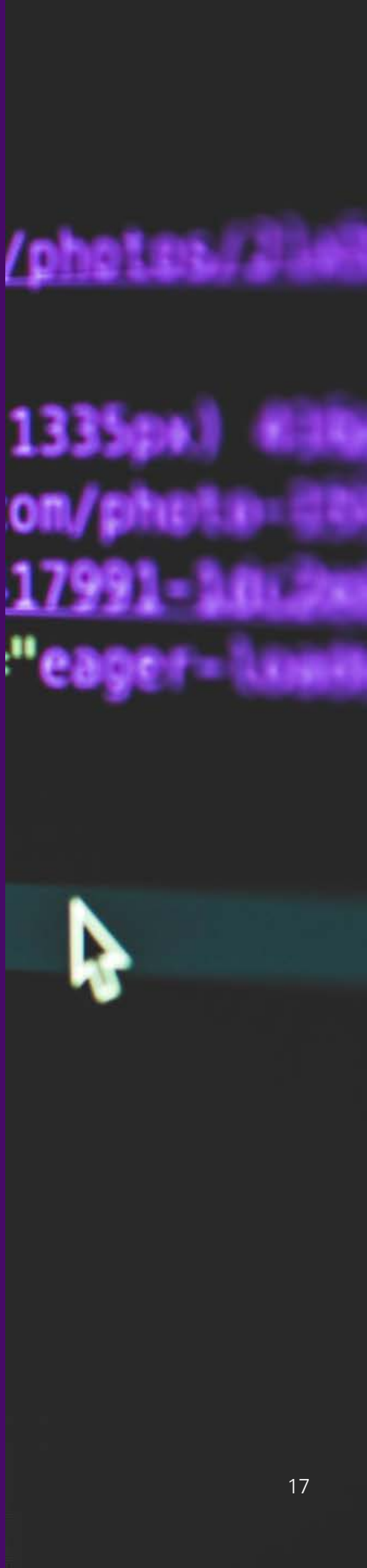
B. Statistics for 2018

C. Proceedings against central register of debtors

Czech act on personal data processing adopted

The new Personal Data Processing Act adapting the GDPR regulation into the Czech legal environment was published in the Collection of Laws under No.110/2019 Coll.

The act deviates from GDPR in a few cases (where the regulation allows). For example, the age limit for parental consent in connection with the provision of information society services was reduced to 15 years. Another deviation is that a Data Protection Impact Assessment (DPIA) does not have to be carried out if the processing of personal data is necessary for compliance with a legal obligation. In such case, it is also entirely sufficient that the data controller fulfils their information obligation towards the data subjects by publishing the information in a manner allowing remote access.



Statistics for 2018

76 inspections were initiated by the Czech Data Protection Authority (in 2017 it was 100)

- 260 personal data breaches were reported under Article 33 of GDPR
- 3616 complaints were received by Data Protection Authority (in 2017 it was 1684)
- 56 fines were imposed in 2018 (in 2017 it was 61)
- The highest fine was CZK 1,500,000 (app. EUR60,000)

Proceedings against Central Register of Debtors

The Central Register of Debtors (CERD) is a private information system, which is often blamed for misleading practices, as it issues certificates of indebtedness which are not accepted by any major financial institution.

The Czech Data Protection Authority carried out an inspection of personal data processing by CERD. Subsequently, remedial action proceedings were initiated and the Authority approached the CERD service provider to shut down its websites. However, CERD found a new service provider, an Indian company that hosts CERD IP addresses from Russia. Therefore, the Czech Authority lost its ability to block the unlawful content.

The Authority has thus initiated sanction proceedings for not taking the remedial measures and is currently preparing a resolution on the matter.

If you have any questions, please let us know

Viktor Dušek
Counsel
KPMG in the Czech Republic
T: +420 222 123 746
E: vdusek@kpmg.cz

Filip Horák
Associate Manager
KPMG in the Czech Republic
T: +420 222 123 169
E: fhorak@kpmg.cz

Ladislav Karas
Associate
KPMG in the Czech Republic
T: +420 222 123 276
E: lkaras@kpmg.cz

OndřejVykoukal
Associate
KPMG in the Czech Republic
T: +420 222 123 660
E: ovykoukal@kpmg.cz

Georgia

A. Core principles and major legislation for the protection of personal data in Georgia

Core principles and major legislation for the protection of personal data in Georgia

Legal Development

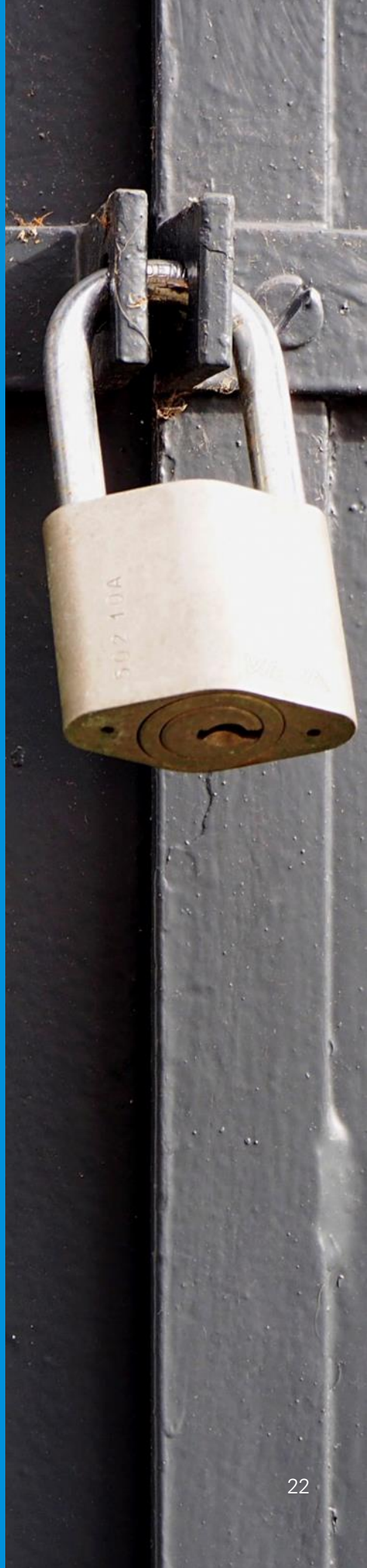
The primary legal act adopted for protection of personal data in Georgia is the Law of Georgia on Personal Data Protection. The Law establishes the rights of individuals and imposes obligations on the personal data processor organizations. The body responsible for the enforcement of personal data protection regulations is the State Inspector's Service.

Background/Issue

The first major step towards the protection of personal data in Georgia took place on 16 January 2012 when the Law of Georgia on Personal Data Protection was adopted. Since then, numerous amendments were adopted to the original version of the Law. The latest amendments in May 2019 replaced the Personal Data Protection Inspector with the State Inspector's Service, which is now responsible for data protection in Georgia.

Impact

As a result of personal data protection regulations, individuals became entitled to request the data processing organizations to correct or update information, block, delete and destruct data. Data controlling or processing organizations are obliged to process data in compliance with a number of regulatory requirements in consideration of a major principle – no data should be processed without due justification of the need for processing such data. In case of infringement of the applicable regulations, the State Inspector's Service is authorized to order the organizations to stop and eliminate violations and to impose monetary penalties.



If you have any questions, please let us know

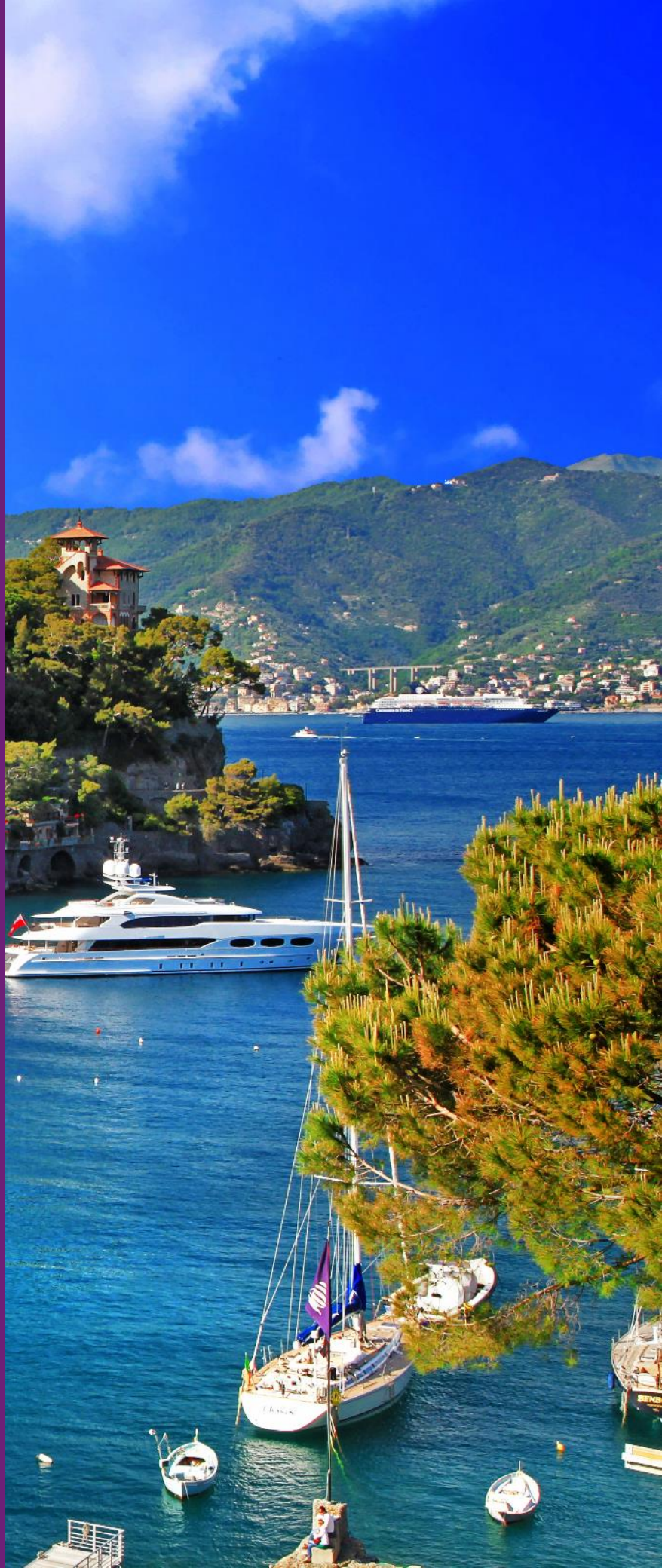
Jaba Gvelebiani
Head of Legal Department
KPMG in Georgia
M: + 995 322 935 713
E: jgvelebiani@kpmg.com

Italy

A. The list of processing operations subject to DPIA as drafted by the Italian data protection authority

B. Data breach

C. Marketing activities & consent



The list of data processing operations subject to DPIA as drafted by the Italian Data Protection Authority

On October 11, 2018, the Italian Data Protection Authority (hereinafter referred to as "IDPA") issued a list containing 12 data processing operations that, if performed, impose on the relevant Data Owner the requirement to execute a specific Data Protection Impact Assessment before starting such processing activities.

Such list has been drafted pursuant to the Opinion n. 12/2018 of the European Data Protection Board (EDPB), with the WP ex art. 29 Opinion no. 248 and to Article 35 (4) GDPR.

Therefore, the IDPA outlined 12 kinds of processing operations which are subject to the requirement:

— Large-scale evaluation or scoring processing, as well as processing involving the profiling of data subjects and the carrying out of predictive activities, including activities online or through apps, relating to "aspects concerning the professional preferences, economic situation, health, personal preferences or interests, reliability or conduct, location or displacements of the data subject";

— Automated processing for the purpose of taking decisions which have 'legal effects' or 'significant similar effects' on the data subject, including decisions which prevent the data subject from exercising a right or making use of goods or service or continuing to be party to an existing contract (e.g. screening of a bank's clients using data recorded in a central risk database);

The list of data processing operations subject to DPIA as drafted by the Italian Data Protection Authority

— Processing involving the systematic use of data for the purpose of observing, monitoring or controlling the data subjects, including the collection of data through networks, whether carried out online or through apps, as well as the processing of unique identifiers capable of identifying users of information society services, including web services, interactive television, etc., with respect to usage habits and viewing data for extended periods. This includes metadata processing, e.g., in telecommunications, banks, etc., carried out not only for profiling, but more generally for organisational reasons, budgetary forecasts, technological upgrades, or to improve networks, as well as to offer anti-fraud, anti-spam, security and other services;

— Large-scale processing of data of a highly personal nature (see WP 248, rev. 01): this refers, inter alia, to data relating to family or private life (such as data relating to electronic communications for which confidentiality must be protected), to data affecting the exercise of a fundamental right (such as location data, the collection of which jeopardises freedom of movement) or whose misuse has a serious impact on the daily life of the data subject (such as financial data which could be used to commit fraud in respect of payments);

— Processing in the context of an employment relationship by means of technological systems (including video-surveillance and geolocation systems) from which it is possible to carry out remote monitoring of employees' activities (see WP 248, rev. 01, in relation to criteria no. 3, 7 and 8);

— Non-occasional processing of data relating to vulnerable persons (children, disabled, elderly, mentally ill patients, asylum seekers);

— Processing carried out using innovative technologies, even with particular organisational measures applied (e.g., IoT; artificial intelligence systems; use of online voice assistants via voice and text scanning; monitoring carried out by wearable devices; proximity tracking such as Wi-Fi tracking) at least one other criteria identified in WP248, rev. 01 applies;

— Processing involving large-scale data sharing between different controllers on large scale using telematics means;

— Processing of personal data by interconnecting, combining or comparing information, including processing activities involving the cross-referencing of digital goods data with payment data (e.g. mobile payment);

— Processing of special categories of data under Article 9 GDPR or data relating to criminal convictions and offences under Article 10 GDPR linked to other personal data collected for different purposes;

— Systematic processing of biometric data, considering, in particular, the volume of data, the duration, as well as the length or persistence, of the processing activity; and

— Systematic processing of genetic data, considering, in particular, the volume of data, the duration, as well as the length or persistence, of the processing activity.

Nevertheless, it is necessary to point out that this revised list drafted by the IDPA is neither to be considered exhaustive, nor directly entailing the obligation to carry out a DPIA, given that the final decision lies, in accordance with the accountability principle, on the data controller's assessment of the presence of a high risk for the rights and freedoms of natural persons.

Data breach

The Italian Data Protection Authority (IDPA) recently stated that the communication to the data subjects following a 'high risk' data breach shall contain all the information concerning the data breach that has occurred and the safety measures to be adopted by each individual in order to minimize the detrimental effects of such an event.

Such clarification arises from the following case: a company communicated to the IDPA that a huge amount of personal data (over than 1.5million of emails, name, surnames etc.) had been stolen from its servers. The company – in the very same data breach communication – stated that all the data subjects would have been duly informed of the data breach.

Following specific investigations, the IDPA discovered that the company did not inform all the data subjects involved in the data breach (only the 50% of them effectively received a communication).

In addition to the above, the IDPA found out also that the standard communication to the data subjects – as drafted by the company – was broadly generic concerning the description of the event occurred and it did not point out both the possible consequences of the data breach and how the data subjects could/should manage the risks related to such event.

The IDPA forced the Company to re-draft such communication, in order to provide full information concerning the data breach to each data subject and to outline all the measures to be taken by the data subjects in order to minimize/prevent the risk of further violations of their rights.

Marketing activities & consent

The Italian Data Protection Authority ("IDPA") has recently pointed out that a customer can not be forced to give their consent to the performance of marketing activities by the relevant Data Owner in order to be allowed to participate in a point accrual programme.

In this sense, the IDPA detected that a renowned multinational company (mainly engaged in the business sector of manufacturing and sale of diapers) had sent over 1 million emails to the participants of one of its accrual programmes.

Investigating on the specificity of the consents obtained by the company, the IDPA discovered that the consent form drafted by the company left no choice for the data subjects to express their consent to specific data processing activities: the data subjects were forced to give a unique, general and non-specific consent to several data processing activities to be performed by the company.

More specifically, if a data subject wanted to participate in the point accrual programme, they were forced to give their consent to all the processing activities outlined by the company without having the opportunity to express their specific consent with reference to each data processing activity.

Consequentially, the IDPA ordered the company to immediately desist from performing any data processing activity on the personal data obtained through the above-mentioned consent form and it fined the company for each single violation (the company has been fined for each email sent without a valid consent).

If you have any questions, please let us know

Dr. Michele Giordano
Managing Partner
Florence, Italy
T: +39 348 6561052
E: michelegiordano@kpmg.it

Avv. Paola Casaccino
Attorney-at-law
Senior Manager Governance, Risk & Compliance Services
Florence, Italy
T: +39 348 4420380
E: pcasaccino@kpmg.it

Avv. Alessandro Legnante
Attorney-at-law
Senior Legal Specialist,
Risk & Compliance Services
Florence, Italy
T: + 39 345 5989855
E: alegnante@kpmg.it

Avv. Giulio Grasso Cannizzo
Attorney-at-law
Senior Legal Specialist,
Risk & Compliance Services
Florence, Italy
T: +39 347 0739460
E: ggrassocannizzo@kpmg.it

Romania

A. 1 year of GDPR in Romania

B. Launching the guidelines questions and answers on the application of Regulation (EU) 2016/679

C. The processing of personal data within the context of parliamentary elections

1 year of GDPR in Romania

The Romanian National Supervisory Authority for Personal Data Processing (hereinafter named "NSAPDP") issued statistics regarding its activity from 25th of May 2018 up to 24th of May 2019.

The following information has been reported:

— During this period 9,439 data protection officers were registered, 398 data breaches notifications were registered, 5,260 complaints were filed, 485 ex officio investigations were concluded and 496 investigations were performed as a result of the complaints filed.

— As a result of these activities performed, NSAPDP issued 57 corrective actions and 23 warnings.

The corrective actions mainly focused on:

— Observing the right to be informed and how it has been enacted;

— Providing complete and legally valid replies without undue delay to data subjects' requests for exercising the right of access;

— the compliance with data protection principles, mainly the lawfulness of processing, the transparency and the proportionality principles;

— implementing adequate technical and organizational measures in order to ensure the security and confidentiality of the data, as well as the observance of these measures;

— erasing the personal data at the end of the relevant retention period set in relation to the purpose for which the was collected.;

— training of the persons working under the authority of the controller (the controller's employees); and

— transmitting commercial messages (marketing) through electronic means of communication only with the prior express consent of the user.

1 year of GDPR in Romania

The complaints received mainly focused on:

— the non-observance of the legal conditions concerning the exercise of the rights of data subjects (e.g.: right to information, right of access, right to objects, right to be forgotten);

— the receiving of unsolicited commercial messages (marketing);

— the disclosure of personal data on the Internet;

— the infringement of the personal data processing principles in connection with the data processing in the banking sector;

— the legality conditions relating to the instalment of video surveillance systems; and

— the infringement of the confidentiality and security rules for the processing of personal data.

The most frequent data breaches involved:

— the unauthorized access to personal data processed by the controller;

— the transmission of the invoices of the controller's customers to a wrong recipient;

— the disclosure of personal data / patients' data; and

— the loss of postal items.

— When compared with 2017, when the NSAPDP received 3,734 complaints, the number of complaints increased significantly, which shows that the data subjects' awareness in respect to their rights also increased.

— The NSAPDP issued its first fine (130,000 Euros) at the end of June 2019.

Launching the guidelines questions and answers on the application of Regulation (EU) 2016/679

The NSAPDP has published on its website Guidelines on the application of the Regulation (EU) 2016/679 which contains 85 frequently asked questions and answers. Of these we mention:

What does "processing operations on a large scale" mean?

When determining whether processing is carried out on a large scale, the following factors must be taken into account: number of the data subjects, volume of data and/or the range of data processed, the duration or the permanence of the data processing activity, and the geographic area of the processing activity.

Is it mandatory to submit to and obtain NSAPDP's approval of a data protection impact assessment performed by a data controller?

The data controller must consult the authority before data processing when the impact assessment indicates a high risk in the absence of measures taken by the controller to mitigate the risk. Also a data impact assessment must be submitted at the request of the NSAPDP when it is performing an investigation.

How do I amend the contact details of the Data Protection Officer included in the on-line form submitted to the authority?

When making changes to the contact details of a Data Protection Officer, it is necessary to file a new on-line form on the authority's website.

How should an investigation be performed by the NSAPDP?

The investigations can be performed on the data controller's/processor's premises, at the authority' headquarters or in writing. The investigation cannot begin before 8 a.m. and cannot continue after 6 p.m., unless the subject of the investigation grants his consent.

When the investigations are carried out at the headquarters of the authority, the subject of investigation must be informed regarding the date and time of the investigation.

In the case of written investigations, a request is sent to the subject of investigation for information, data and documents necessary to resolve the case under investigation.

The processing of personal data within the context of parliamentary elections

In the context of the European Parliamentary elections in May 2019, the National Supervisory Authority recommended that all entities involved in this process pay a greater attention to compliance with personal data protection legislation to ensure that personal data are used in a responsible way and that the rights of data subjects are respected.

The GDPR provides in Article 6 when processing is lawful.

In addition, we mention that Article 5 of the GDPR establishes a series of principles which shall be observed when processing personal data.

These include, among others, the principle according to which the data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("purpose limitation") and personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures ("integrity and confidentiality").

Also, the same legal provisions mentioned above state that the controller shall not only be responsible for complying with these principles, but also be able to demonstrate compliance with these principles ("accountability").

At the same time, according to the GDPR provisions, the controller involved in the electoral process has the obligation to respect the rights of the data subjects, in particular the right to information regarding the processing of personal data.

Please note that the GDPR does not impose a certain way of informing the data subjects, leaving it to the controllers to choose effective ways of providing the information – posting on the site, on the notice board, in writing etc.

By Regulation (EU, Euratom) no. 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations, the European Authority for European Political Parties and Foundations was established for the purpose of recording, controlling and imposing sanctions on European political parties and European political foundations.

Article 10 let. a) of the above-mentioned Regulation provides the authorities with a verification procedure in respect of infringements of the rules on the protection of personal data by political parties and foundations.

Regarding these aspects, within the context of the elections for the European Parliament and other EU elections planned for 2019, the European Data Protection Board adopted Statement 2/2019 on the use of personal data in the course of political campaigns. These underline a series of key points to be respected when political parties process personal data in the course of electoral activities.

In light of the above, we emphasize the need to respect the rules on the protection of personal data, including in the context of electoral activities and political campaigns.

If you have any questions, please let us know

Adrian Lincă
Legal Consultant
KPMG in Romania
T: +40 (728) 008 138
E: alinca@kpmg.com

Laura Toncescu
Partner KPMG, Head of KPMG Legal
KPMG in Romania
T: +40 (728) 280 069
E: ltoncescu@kpmg.com

Spain

A. The Spanish Data Protection and Digital Rights Guarantee Act

B. The first significant fine by the Spanish Data Protection Authority: "La Liga"

C. Political parties and profiling

The Spanish Data Protection and Digital Rights Guarantee Act

Following the date of application of the GDPR, as per Article 99 thereof, a new Data Protection law (Constitutional Act 3/2018, of 5 December, on Protection of Personal Data and Guarantee of Digital Rights) (hereinafter referred to as "LOPDGDD", its Spanish acronym) was published in the Spanish Official State Gazette on December 6 and entered into force on 7 December 2018.

Spain is a country with a great heritage in the field of data protection. The Spanish Constitution of 1978 states in its Article 18.4 that "the law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights". In line with this mandate, the Spanish legislator passed the first data protection act back in 1992 and created and funded a supervisory authority, which has proven to be very active and protective over the years.

The LOPDGDD is not aimed at adapting the Spanish privacy regulatory framework to the GDPR but only at supplementing and providing interpretation to some of its precepts. The LOPDGDD provides guidance for compliance with a number of GDPR key questions:

- Concerning the provision of information to the data subjects, it sets the minimum information that has to be provided in a first layer.
- Concerning the nature and features of consent, it allows "all in" consent collection formulas. The controller must request the specific consent of the data subject for each processing purpose, but can also provide the data subject with a system to accept all the requests with a single action.
- Concerning the applicable legal basis for the processing, it sets forth a number of (iuris tantum) assumptions where the processing of the data can rely on legitimate interests of the controller.
- Concerning the exercise of the right to restrict the processing or situations where the data is retained longer than necessary for the purposes for which they were collected, it sets forth an additional obligation: the blocking of the data.
- Concerning the credit information systems, it sets forth a minimum financial limit for the inclusion of personal data in these systems, which should help to avoid the stigmatization of debtors.
- Concerning the processing of health related data, it provides a list of sector regulations which cover health data processing activities which shall be deemed to rely on the exception contemplated in Art. 9.2 g) of the GDPR.

In addition, it also introduces a set of digital rights, such as the right to universal access to the Internet, to digital disconnection, digital education, digital security, amongst others.

Spanish Data Protection Authority fine on Spanish football league "La Liga"

According to the press release published by the Spanish Professional Football Association ("La Liga"), the Spanish Data Protection Authority has imposed a fine of EUR 250,000 for violation of the principle of transparency towards data subjects in respect of the information provided to the users of its official mobile application. Until the decision is published, the information on the infringement is limited and refers to the use of the mobile's microphone and the geo-location functionality to detect illegal screenings and combat piracy in bars and similar establishments where football matches were broadcasted.

La Liga has announced that it will appeal the sanctioning decision in court. It alleges that the users had to provide their consent twice for activation of the microphone and that only a very limited amount of data were processed.

This case may clarify the scope and amount of information that needs to be provided to the data subjects (both in a first and second layer) for consent collection purposes.

Political parties and profiling

Article 58 bis of the Spanish General Electoral System Act, relating to the "use of technological means and personal data in electoral activities" was amended by the Spanish Data Protection Act (Final Provision 3) to allow "the collection [and processing] of personal data related to political opinions […] by political parties in the framework of their electoral activities" on the basis of public interest, provided that adequate safeguards are provided.

This was an extremely controversial measure, heavily contested by both the legal authors and the public.

The adopted provision allowed political parties to gather information posted on social networks to make ideological profiling during election periods without the data subject's consent. In fact, this provision was against a general rule contained in the Spanish Data Protection Act by means of which, not even the consent of the data subject (by itself) is considered to legitimate data processing the main purpose of which is to make an ideological profiling of the data subject (Art. 9.1 of the LOPDGDD).

The Spanish Data Protection Authority's approach was that Article 58 bis of the Spanish General Electoral System Act "does not protect the application of big data or artificial intelligence technologies to infer a person's political ideology, as this would be a violation of his fundamental right not to declare his ideology".

In line with this stance, the Spanish Ombudsman filed an appeal before the Constitutional Court requesting that the aforementioned article was declared null and void. It defended that it violated the right to ideological freedom, to the protection of personal data, to the freedom of expression and to political participation.

The Constitutional Court upheld the appeal, declaring contrary to the Constitution and consequently null and void Article 58 bis of the General Electoral System Law. This decision was adopted after the general elections to elect the Spanish Parliament that took place on 28 April 2019.

If you have any questions, please let us know

Bartolome Martin
Director
IP & Technology
KPMG in Spain
T: +34 91 4563400
E: bartolomemartin@kpmg.es

Eric Romero
Senior Associate
IP & Technology
KPMG in Spain
T: +34 93 2532900
E: ericromero@kpmg.es

UK

A. Brexit planning

B. ICO report

Brexit planning

Even taking into account the possibility of further delays to the Brexit process, it is recommended that companies take steps to prepare themselves for the possibility of the UK leaving the EU on 31st October 2019.

The ICO has offered the following guidance for companies:

1. Ensure continued compliance with current standards of Data Protection legislation:
    a. The UK government intends to incorporate the GDPR into UK law on exit, and it will sit alongside the existing Data Protection Act 2018.
    b. Current guidance will largely remain relevant.
2. Transfers of data into the UK:
    a. Companies should review their data flows and identify where they receive data from the EEA, including from suppliers and processors.
    b. If the EU makes a formal adequacy decision regarding the UK's regime, there will be no need for specific safeguards.
    c. Failing that, plans should be put in place to ensure adequate safeguards are implemented.
3. Transfers of data out of the UK:
    a. Following step 2 above, a review of data flows should also reveal where data is flowing out of the UK into the EEA.
    b. Data flowing from the UK to the EEA will likely not be restricted, as rules governing data flows from the UK to countries outside the EEA will remain similar.
4. Companies with European Operations:
    a. Companies operating across Europe will need to perform a more detailed review of their data flows.
    b. They may find that they have compliance obligations under both EU and UK law and that they will be held accountable to both the UK and EU regulators.
    c. Companies that currently have the UK's ICO as their lead supervisory authority will need to reassess their situation to benefit from One-Stop-Shop.
    d. A European representative may need to be appointed.
5. Changes to Documentation:
    a. Privacy information and associated documentation will need to be reviewed and updated to reflect that the UK has left the EU.
6. Maintaining Awareness:
    a. Companies should maintain awareness of the need for compliance and the impact of Brexit.

ICO report

The ICO has published a report on its reflection of the GDPR one year on.

The ICO provides support and guidance and also enforces the GDPR, acting in the public interest when organisations break the law.

Enforcement and the Regulatory Action Policy (the "Policy"):

In enforcement the ICO's general objectives are to:

- Respond to breaches quickly and efficiently.
- Focus on the most pressing breaches e.g. those involving large groups of adversely effected individuals or those impacting vulnerable individuals.
- Impose consistent sanctions.
- Concentrate the most significant powers on organisations/individuals repeatedly failing to protect personal data.
- Support compliance with the law through information sharing, promoting good practice and advising on how to comply.
- Identify and mitigate new or emerging risks arising from technological and societal change.
- Work with other regulators and interested parties to recognise and monitor the nature of the technological landscape and the way in which data flows in the digital economy.

The Policy also focuses on how the ICO will use their powers to uncover and address processing which has attracted increased public attention and concern. Examples of such include social media companies and political parties.

The ICO is using its powers to change behaviours and ensure that individual rights are upheld. One example being:

- Recent action against HMRC for failing to obtain customer consent to use their voices in recognition software, resulted in the ICO issuing an order requiring HMRC to delete the records of five million individuals.

New powers of inspection have enabled the ICO to respond to public concerns about unsolicited marketing communication. In addition, the ICO has issued 15 assessment notices under the new law in conjunction with investigations into data analytics for political purposes.

Statistics

25 May 2018 – 1 May 2019

The ICO received approx. 14,000 reports of personal data breaches ("PDB") reports, a significant increase on the year starting 1 April 2017 in which approx. 3,300 such reports were received.

12,000 of the 14,000 cases were closed during the year.

- 82% required no action.
- 17.5% required action form the organisation.
- Less than 0.5% led to an improvement plan or monetary penalty.

ICO believes that this indicates that:

- Businesses are taking requirements of the GDPR seriously
- However, it remains a challenge for organisations and Data Protection Officers ("DPO"s) to assess and report all breaches within the statutory timescales.

ICO report (cont.)

Public Data Protection Concerns:

The number of concerns raised by the public has increased.

25 May 2018 – 1 May 2019

— The ICO received over 41,000 data protection concerns from the public, compared to 21,000 for 2017/2018.

- Most frequently these are about subject access requests, as was the case pre-GDPR.
- However the general trend is that all categories of complaint have increased.

Sectors:

The sectors responsible for higher numbers of PDBs and data protection concerns are as follows:

— Health sector

— Local governments

— Lenders

This knowledge helps the ICO to target further guidance, support and action

International:

25 May 2018 – 1 May 2019

Out of the 240,000 cases that were received by the EU Data Protection Board, the ICO received over 55,000 (approx. 23%).

The Information Commissioner was elected as chair of the International Conference of Data Protection and Privacy Commissioners – this role gives the UK a leadership role within the sphere of global privacy and information rights.

Volume of contact with the ICO and DPOs:

There has been an increase in the volume of contact with business, organisations and individuals.

— ICO's helpline, live chat and written advice services received over 470,000 contacts in 2018/2019 which is a 66% increase from 2017/2018.

The ICO wants to see DPOs embedded and supported in their respective organisations by senior management. It is critical to the success of DPOs to have engagement from board level.

Innovation: Developing Sandbox

The ICO is developing its Sandbox, a new service designed to support organisations using personal data to develop products and services that are innovative and have demonstrable public benefit. This will enable participants to work through how they use personal data in their projects with specialist staff from the ICO to ensure compliance.

If you have any questions, please let us know

Lucy Jenkinson
Solicitor, ISEB (Data Protection)
KPMG in the UK
T: +44 (0) 131 527 6823
M: :+44 (0)7825089364
E: Lucy.Jenkinson@KPMG.co.uk

Lydia Simpson
Barrister, BCS (Data Protection)
KPMG in the UK
T: +44 (0)20 7311 8865
M: +44 (0)7810056806
E: Lydia.Simpson@KPMG.co.uk

Emma Cartwright
Solicitor
KPMG in the UK
T: +44 (0)20 7694 4147
E: Emma.Cartwright@KPMG.co.uk

*KPMG LLP is a multi-disciplinary practice authorised and regulated by the Solicitors Regulation Authority.

kpmg.com

Designed by CREATE | CRT115985 | June 2019