Data privacy newsletter

KPMG Global Legal Services

June-July 2020

Contents

KPMG

Introduction

Welcome to the fifth edition of 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 the responses of Data Protection Authorities from various jurisdictions to the COVID-19 situation, decision regarding data protection officers, cyber attacks on hospitals, guidelines for video conferencing systems, recent data breaches, annual report of certain Data Protection Authorities.

KPMG

Argentina

A. COVID-19: Handling of sensitive data

COVID-19: Handling of sensitive data

Health-related information is considered sensitive information by the Argentine Data Protection Law. Measures adopted as a consequence of the COVID-19 spread aimed at monitoring people's health shall consider sensitive data regulations.

The Argentine data protection authority, Agency of Access to Public Information, issued the following recommendations based on Argentine Data Protection Law, the DPL, when processing personal data related to COVID-19:

- Health data falls under the category of sensitive data, being subject to more rigorous protection;
- In case of testing positive to COVID-19, the patient's prior consent is necessary to communicate his/her name;
- Health institutions and doctors can process and share between themselves personal data of their patients provided they keep such data confidential;
- The obligation of professional secrecy remains even after the relationship with the patient is over;
- It is necessary to obtain the patient's prior consent to use his/her health information with purposes different from the ones for which it was collected;
- The National Health Ministry as well as the Provincial Health Ministries are authorized to request, collect, transfer to each other or process in any other way health information without the consent of the patients, in accordance with the explicit and implicit powers that they have been given by law.

Notwithstanding the foregoing, employers in certain specific circumstances may be exempted from collecting the consent of the employee who is COVID-19 positive, in order to adopt the necessary measures to prevent new infections, and therefore fulfill the employer's duty to prevent damages related to the pandemic.

COVID-19: Handling of sensitive data (cont.)

The Argentine Government has also shared the Executive Committee of the Global Privacy Assembly's statement on global recommendations for personal data processing: "health related information are considered sensitive in many jurisdictoins, but the work among data protection authorities and Governments have shown many examples of national approach to share messages of public health, the use of the latest tecnnology to facilitate consultation and safe and rapid diagnosis; as well as to create links among public information systems in order to enable the identificaton of the COVID-19 spread."

The Committee is confident that data protection requirements will not stop the critical sharing of information to support efforts to tackle the global pandemic, and that the universal data protection principles in all our laws will enable the use of data in the public interest and still provide the protection the public expects. It is worth mentioning that the Director of the Argentine Agency of Access to Public Information is a member of the Excecutive Committee of the Global Privacy Assembly.

In connection to this, the Administrative Decision No. 431/2020 of the President's Chief of Staff Office states that "the capacity of the State to have relevant information for the purposes of public health care, in a timely manner and within the regulatory framework in force, stands as an essential and indispensable asset for decision-making "

Therefore, the entities within the Argentine Public Sector are authorized to transfer, assign, exchange or in any way make available the data and information that, because of their powers, missions and functions, are in their files or databases. This must be performed in accordance with the technical and organizational measures that are necessary to guarantee security, confidentiality and processing in order to protect public health.

Accordingly, the DPL sets forth that personal data may be transferred without the consent of the data subject when it is collected within the scope of the powers of the State when exercising its functions, and allows the possibility of carrying out mass transfer of personal data between State agencies directly, provided it is done in compliance with their respective powers.

As regards labour relationships, the employer should evaluate whether the company has adequate security levels to be able to process sensitive information and guarantee their integrity. It should also analyze whether there are any privacy restrictions to inform within the company, the company group, or with the medical, health and/or security authorities those employees who have tested positive for COVID-19. The employer should check if it has collected the relevant consent forms to enable asking employees about their plans to travel or where they have recently been, to measure employees' temperature or make them undergo medical examinations. The employer should evaluate if new consent forms should be collected from employees to allow the processing of such information.

COVID-19: Handling of sensitive data (cont.)

Geolocation application

The Argentine Ministry of Health, the MoH launched an app named Cuidar which collects - among other information - geolocation information from its users to recommend steps to follow according to the symptoms that were entered therein, and to make comparisons or predictions based on the MoH's sanitary recommendations. The MoH can use the information uploaded to the app to map risk areas, as well as areas where social distance cannot be attained that could increase the spread of the virus.

In accordance with the provisions of the DPL, a data base corresponding to the app Cuidar has been created and published in the Official Gazette. Moreover, the Agency of Access to Public Information published on its website certain recommendations for the use of the app, recalling that, in accordance with the applicable law for the protection of personal data in Argentina, the monitoring of the location of individuals is not prohibited, provided that such monitoring is carried out respecting the human right to privacy.

In this regard, the Agency lists fundamental principles on data protection applicable to geolocation tools, which include the following:

- Information regarding a person's location and/or movements constitutes personal data protected by law. Its processing must have a valid legal basis.
- The dissociation of location data excludes the application of the DPL, as it does not qualify as personal data.
- Geolocation data may be processed by State agencies without the consent of the data, provided it is performed within their specific powers – which must be interpreted in a strict and restrictive sense. Otherwise, State agencies must resort to the consent of the data subject in order to be able to process his/her information with a valid legal basis. The same principle applies to transfers of data between State agencies.
- The data subject must have the possibility to revoke his/her consent to monitoring at any time.
- The data quality principle set forth in the DLP is applicable; according to which the information collected (location) must be true, relevant and not excessive in relation to the purpose of its collection.
- The data subject must be informed on how and why the data is being monitored, where the information is stored, with whom it is shared, the consequences of the processing and the possibility for the data subject to exercise their rights of access, rectification or deletion.

Finally, the Agency also recommends carrying out a privacy impact assessment prior to the implementation of these types of tools to control and mitigate the risks, as well as to assess the feasibility thereof.

Argentina

If you have any questions, please let us know

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

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

María Lucila Celario
Consultant
KPMG in Argentina
T:+541143165700
E: mcelario@kpmg.com.ar

Belgium

A. The Belgian DPA's response to COVID-19

B. First decision regarding a DPO

Belgium

The Belgian DPO's response to COVID-19

Given the topical issue of COVID-19 and its impact on data protection, the Belgian Data Protection Authority (BDPA) has decided to publish on its website a number of guidelines to provide clarifications on a Belgian level.

Firstly, the BDPA emphasized the GDPR's applicability in **employer-employee relationships** under the current circumstances. When companies or organizations take certain measures to help combat COVID-19 involving the processing of personal data, the provisions of the GDPR must always be taken into account. At the same time, however, protecting personal data may not limit the battle against the spread of the virus, according to the BDPA.

The following recommendations were made over the course of the last months:

— In regards to the lawfulness of processing, there is currently no reason to base any processing of personal data on the 'protection of vital interests' of the data subject or another natural person in Belgium (article 6.1(d) GPDR);

— Processing health data is principally prohibited as it classifies as a special category of personal data unless an exclusion ground applies (article 9 GDPR);

— Performing systematic temperature checks on visitors and employees is permitted insofar no additional data is registered;

— Requiring employees to fill in a medical questionnaire is prohibited. However, it may be permitted to encourage employees to inform the company doctor of any symptoms and recent travels to unsafe areas; and

— Announcing the name of an infected employee is prohibited, given the principles of integrity and confidentiality (article 5.1(f) GDPR) as well as the requirement of data minimization (article 5.1(c) GDPR). However, it is allowed to inform other employees of an infection within the company or organization without further details. Furthermore, the identity of the infected employee may be communicated to the company doctor and competent government services if required.

The Belgian DPO's response to COVID-19 (cont.)

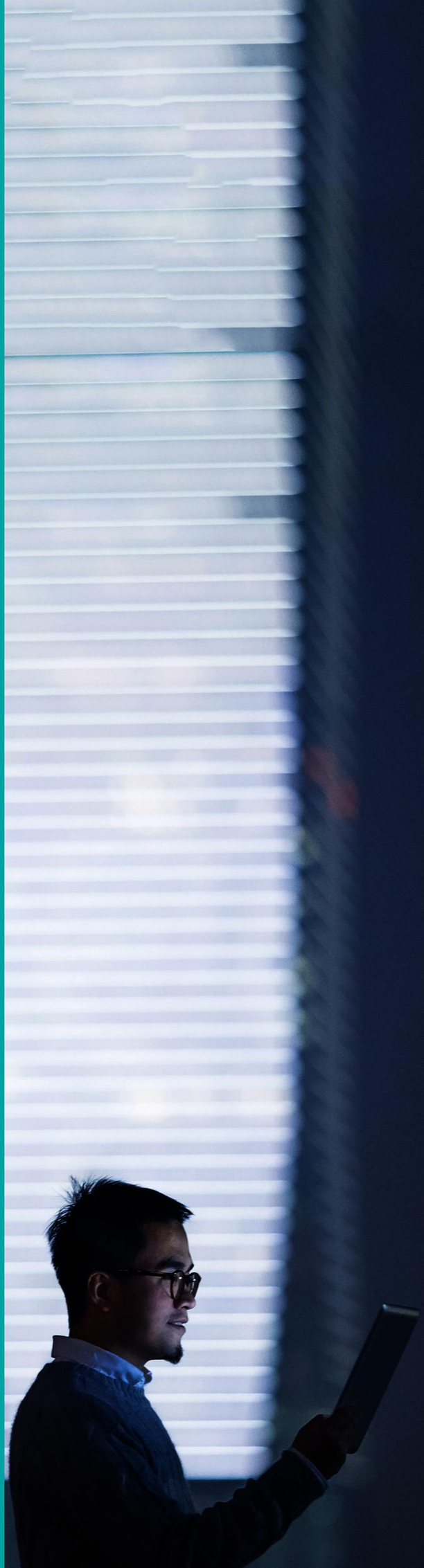
Secondly, the BDPA has clarified some misconceptions in the development and use of **eHealth applications**. *Among others,* the following principles must be adhered to:

— Personal data may not be processed unless it is required for beneficial use. In any other event, no personal data of the user may be requested and strict anonymity must be maintained at all times;

— If the app is used within an existing care relationship between a healthcare provider or institution and patient, this must be explicitly stated. Personal data may only be processed in the qualitative context of providing continuous care by the provider or institution; and

— In case the above advice does not apply, the BDPA provided an overview of the applicable GDPR requirements to comply with when developing eHealth apps.

.



Belgium

First decision regarding a DPO

On 28 April 2020 the Belgian data protection authority (BDPA) has issued an administrative fine relating to a wrongful appointment of a data protection officer (DPO).

The litigation chamber of the BDPA has recently issued a judgement imposing an administrative fine of 50,000 EUR on an organization having appointed a DPO in violation with certain principles of the GDPR.

.

The DPA initially started its investigation due to a data breach within the organization. The inspection report indicated that the organization allegedly made three serious infringements on the provisions of the GDPR, namely:

- **Non-collaboration with the supervisory authority (art. 31 GDPR);**
- **Non-compliance with the accountability principle (art 5.2 GDPR); and**
- **Non-compliance with the obligation to avoid a conflict of interest for the appointed DPO**.

In its judgement, the litigation chamber of the BDPA only upheld the alleged infringement relating to the 'conflict of interest'.

The BDPA stated that the DPO had a conflict of interest due to his other "executive positions" within the organization (i.e. head of Compliance, Risk & Management and internal audit).

The fact that these executive functions did not give the DPO any decision-making powers relating to the data processing activities does not necessarily mean that these executive functions can be combined with the mandate of DPO, according to the BDPA in its judgement.

In addition, the DPA stated that a conflict of interest needs to be evaluated on an 'ad hoc' basis and concluded that in this case – as head of the Compliance, Risk & Management and Internal Audit Department – the DPO had an impact on how the processing of personal data would be performed (i.e. determining the purpose and means of the processing activities) and that this is not in line with the Guidelines for DPO's of Working Group 29.

First decision regarding a DPO (cont.)

In light of these elements the litigation chamber of the BDPA ruled that the organization should resolve the matter within a period of three months and pay an administrative fine of 50,000 EUR. The BDPA justified the amount of the administrative fine based upon the following elements:

— The function of a DPO already exists for several years; and

— The organization should have made the necessary preparations given the fact that the processing of personal data was a core business activity of the organization and the processing takes place on a very large scale; and

— The infringement already started as of 25 May 2018.

The decision of the BDPA shows the importance of the independence of the DPO function within an organization. This decision might be appealed before the Market Court ('court of appeal').

Belgium

If you have any questions, please let us know

Tim Fransen
Senior Counsel
K Law Belgium
T: +32 (0)3 8211809
E: timfransen@klaw.be

Mathias De Backer
Senior Associate
K law Belgium
T: +32 (0)3 8211816
E: mdebacker@klaw.be

Matthias Bruynseraede
Junior Associate
K law Belgium
T: +32 (0)3 8211977
E: mbruynseraede@klaw.be

Czech Republic

Czech Republic

FAQs regarding the coronavirus situation by the Czech DPA

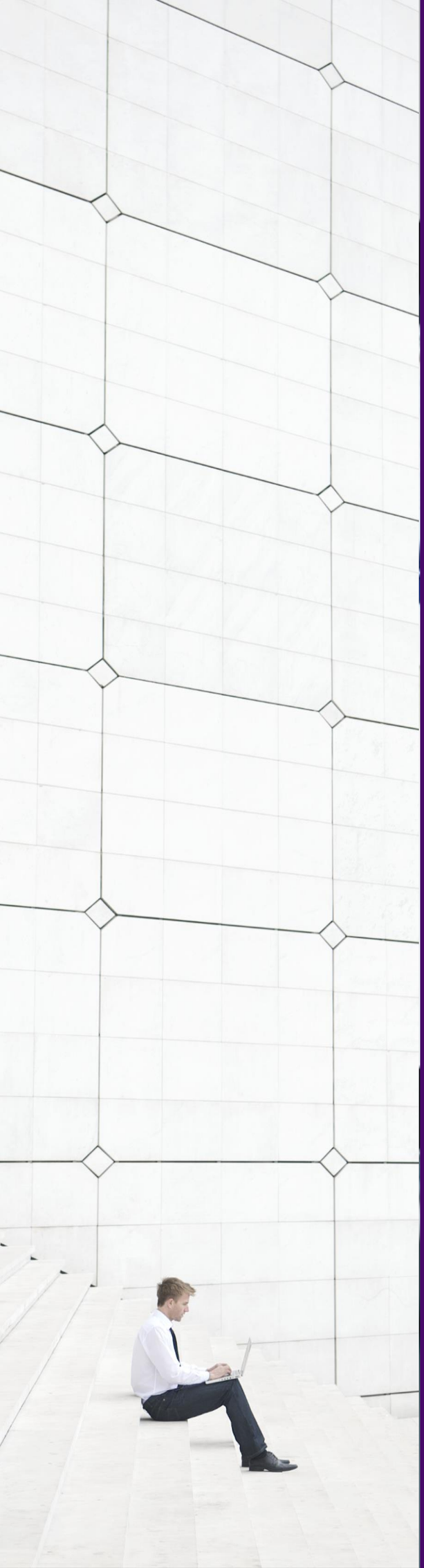
The Data Protection Authority published answers to the most frequently asked questions with respect to the processing of personal data related to the pandemic. Most of them relate to the processing of personal data by public authorities in connection with the extraordinary measures in place. However, one of the answers is relevant to all employers, so we decided to highlight it.

Question: '*In the current situation, can the employer obtain data on the health of employees, for example when recommencing work?'*

Answer: *'In general, the Labor Code obliges employers to create a safe and non-hazardous working environment and working conditions by appropriate organization of occupational health and safety and by taking risk prevention measures.*

In particular situations, the employer is obliged to prevent, eliminate or minimize the risks. The employer is therefore obliged, in the situation of an emergency, to take the necessary protective measures appropriate under the circumstances. It is advisable to proceed in cooperation with public health protection authorities, to which the employer is also obliged in some situations to report facts stipulated by legal regulations.

Moreover, employers must, as a precautionary obligation, inform other employees of the risks appropriately. Such a risk may consist of the presence of an infected person at the workplace. In such case the employer proceeds by taking all necessary measures. Facts about a specific person should be communicated by the employer to the extent necessary for the protection of health only, and so that the dignity and integrity of the person is not affected.'



Czech Republic

Translation of the EDPB's opinion adopted in connection with the COVID-19 outbreak

The Czech Data Protection Authority published a translation of the European Data Protection Board's opinion on the processing of personal data in connection with the outbreak of COVID-19 which was adopted in the second half of March.

The EDPB in its opinion acknowledges that monitoring the incidence of coronavirus infection by using modern technology is in the interest of all mankind. However, even in this extraordinary period, care must be taken to ensure that data subjects' personal data are adequately protected. *'A state of emergency is a circumstance that can legitimize restrictions on freedoms, provided that these restrictions are proportionate and limited to the duration of the emergency.'*

The translation in the Czech language is available here.

Czech Republic

Czech DPA comments on the smart quarantine project

The Authority provided its opinion on certain aspects of the 'Smart Quarantine' program, ordering mobile operators and banks to process data on the movement and behavior of persons infected with the coronavirus.

The basis for the personal data processing is the extraordinary measure of the Ministry of Health and the procedures stipulated in the Public Health Protection Act. According to the Czech DPA, the processing must only cover the necessary operations, which must be carried out within the defined purpose, i.e. to determine an infection's possible source and prevent further spread.

Data gathered must only be kept for the shortest time necessary; according to the Authority, for non-anonymized data, this means a maximum of six hours. Thereafter, the data must be deleted or fully anonymized, to prevent abuse. The Authority has also called on the data controllers (namely the Ministry of Health and the emergency committee) to properly inform the public to dispel any fears of possible breaches of privacy.

Czech Republic

Rules and recommendations for working from home

The Czech Data Protection Authority summarized basic rules and recommendations as regards personal data protection when working from home.

The Authority warned against fraudulent e-mails containing attachments or links that may appear to be important information about the new coronavirus. It has pointed out that personal data should not be transferred through public Wi-Fi networks but via mobile data or VPN which are safer. The Authority also recommended being careful when using passwords, including hard disk encryption.

Employers should develop specific procedures to address any security incidents in a quick and efficient manner. The Authority also offered a reminder that even during the pandemic, employers still have the duty to report any breaches of personal data protection to the Czech Data Protection Authority within 72 hours.

Czech Republic

Czech DPA reacts to the proposed regulation of violence at football stadiums

The Authority commented on the current proposal for adopting new measures against violence at football stadiums using the automated processing of biometric data.

The Authority pointed out in particular that any proposal on the use of biometric technology and automated evaluation of biometric data must include a detailed justification, including a personal data protection impact assessment (DPIA) when it comes to large-scale processing of special categories of personal data. As the use of such technologies would affect all visitors to the sports facility at each sporting event, it is a clear example of processing for which the DPIA is necessary.

The legislative measures must also be followed by technical and organizational measures of the owners and operators of stadiums and organizers of sporting events. As examples can serve the consistent logging of all security record operations or the specific treatment of records in the processing contract under GDPR if the stadium owner or operator entrusts the processing of the biometric data of visitors to a security agency as processor.

The Authority already discussed the possible measures against violence at football stadiums in August last year and did not support the processing of biometric data as it did not find any appropriate legal entitlement to do so.

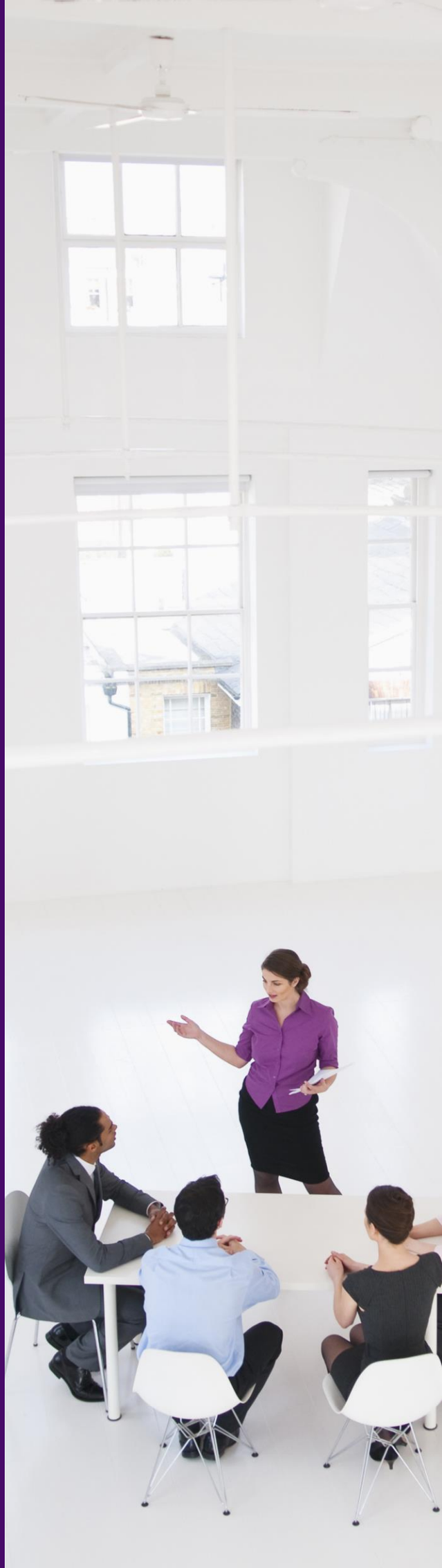
Czech Republic

Statement of the DPA on the personal data of litigants in Internet databases

The Authority has recently dealt with the issue of taking over and further disclosing personal data of litigants in Internet databases. The personal data were processed in a way which enabled the retrospective de-anonymization of court resolutions published by courts in anonymized form. This procedure used data of litigants after the purpose for which they had been disclosed elapsed and thereby infringed their right to privacy.

It is clear from the Authority's decisions that the practice of compiling databases of court decisions which serves to analyze the decision-making activity of courts and contributes to the public control of the judiciary has not been questioned.

However, the Authority assessed the matter of unrestricted and widespread publication and storage of personal data of particular participants in court proceedings. According to the Authority, the rules on personal data protection do not allow the creation and publication of Internet databases whose sources are databases which have been set up and made available for a defined purpose and for a limited period of time only. Therefore, the conclusion is that published personal data cannot be used indefinitely and must be protected.



Czech Republic

Liability of company ordering commercial communications

The Czech Data Protection Authority dealt with the activities of a company which ordered the distribution of commercial communications from an entity abroad. This distributor then promoted the company's services, including sending commercial communications to e-mail addresses without having any consent or other legal entitlement to do so.

The Authority decided that there is strict liability of the ordering entity for the dissemination of commercial communications which cannot be waived by any contractual transfer of responsibility to a third party. The company filed a lawsuit against this decision. Recently, the Municipal Court in Prague dismissed the action.

According to the court resolution, the person distributing commercial communications by electronic means is not only their direct sender but also the person who initiated the distribution, gave an order to do it or profited from it. If the company ordering the distribution was in the position of the data controller, it was its duty to ensure that the personal data is processed in accordance with the applicable laws on the protection of personal data. The company cannot waive or transfer its liability for an administrative offense even when using a third party to carry out the distribution.

Czech Republic

Cyberattacks on hospitals

Following a major cyber security incident which occurred in one of the hospitals in the Czech Republic, the National Cyber and Information Security Agency instructed selected entities operating in the field of healthcare to perform necessary actions that will lead to the security of important information and communication systems against cyber security incidents. The implementation of the set of measures is mandatory for entities to which it has been delivered. The aim of the reactive measures is to minimize the risk of other similar incidents and to prevent possible complications that could occur during the already difficult situation caused by COVID-19.

The Agency also issued a warning against the high risk of serious cyberattacks on information and communication systems in the Czech Republic. According to the Agency, the cyberattacks can have serious impacts on the availability, confidentiality or integrity of information in such systems. The Agency issued supporting material containing recommended measures to be adopted, which specifies procedures for administrators of information and communication systems falling under the Czech Cyber Security Act and provides some additional recommendations.

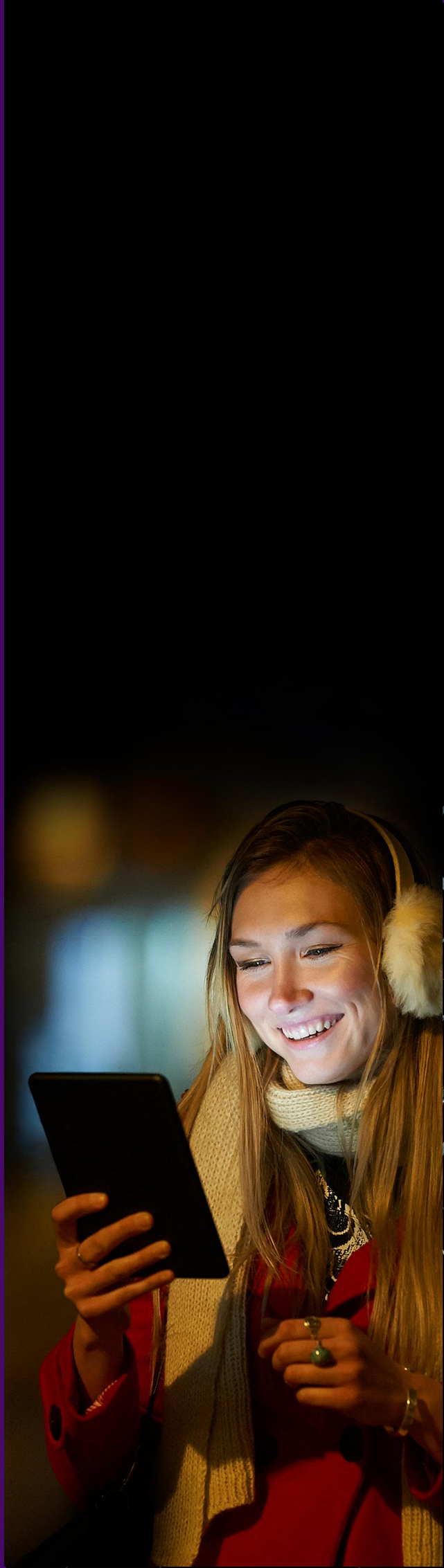
Czech Republic

Warning regarding the security of online conferencing services

The National Cyber and Information Security Agency warned against the vulnerability of online communication, and particularly mentioned Zoom video conferencing services, which has become a very popular solution during the current pandemic situation. The Agency reported that this service is currently a frequent target of attacks, attempts unauthorized connection to the call (so-called *Zoombombing*), and it has recently discovered serious vulnerabilities in Windows and MacOS, which potentially allowed attackers unauthorized access to the target computer. These vulnerabilities should already be fixed in the current version but can still apply to the older versions.

The Agency thus recommended careful consideration of the use of the service for communicating sensitive information. Moreover, the communication within Zoom is encrypted, but not directly between the communicating parties, but between the user and the Zoom servers. Zoom declares that it does not have the means to decrypt or access the calls. However, the communication cannot be considered 100% confidential. In addition, vulnerability with respect to ID generating was mentioned which could allow unauthorized users to enter foreign conferences, but this issue has already been resolved.

The Agency generally recommended being cautious when communicating remotely and, if possible, using reliable end-to-end encryption.



Czech Republic

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

Germany

A. German Data Protection Authorities publish guidelines for video conferencing systems

B. Court restricts right of access in case of disproportionate effort

C. Data protection: ongoing infringement procedure against Germany

German Data Protection Authorities publish guidelines for video conferencing systems

During the COVID-19 pandemic, even more companies are faced with the challenge to cooperate without personal contact. One very practical and effective solution is the implementation of a video conferencing system. For this purpose, German Data Protection Authorities have given advice on how to comply with data protection laws in this regard.

Whether by mere attending a digital conference or by discussing issues while communicating via video conferencing, personal data, such as names, contact information or time and date of the participation or even sensitive data might be generated and collected. Companies are responsible for the protection of the personal data of their employees and clients generated and processed by their digital conferencing systems. Therefore, providers of these digital services have to be selected carefully. Technical aspects as well as legal issues should be taken into consideration. The following abstract highlight the most important topics.

Firstly, in the selection of digital providers, the controller (which regularly is the company implementing and using the system) should ensure that metadata and content data are not analyzed for internal purposes or transferred to third parties.

Further, controllers should use software solutions "on premise", i.e. operated by the controller itself on internal servers and engage only reliable service providers. The advantage of these "on premise" solutions in contrast to the use of external servers is that the controller maintains complete physical control of the personal data generated. However, due to the lack of knowledge or financial resources, not every organization is able to afford such a solution. As an alternative, the controller can engage reliable service providers who provide hosting and maintaining services for the software solution. In this case, a data processing agreement needs to be concluded which includes a provision that prohibits metadata and content data to be analyzed for internal purposes or transferred by the service provider.

If a service provider is engaged, the controller needs to decide whether to commission a service provider (i) with registered office in the European Economic Area (EEA), (ii) in a country with an equivalent level of data protection accepted by the EU, (iii) an US-American provider that is certified according to the Privacy Shield (even though some established US-American providers are considered critically regarding the user's privacy by the German Data Protection Authorities) or (iv) a provider with registered office beyond these protected areas. German Data Protection Authorities recommend engaging European digital providers. In addition, attention should be paid to the place of business of further sub-suppliers of the service provider that might be located outside the EEA.

Germany

German Data Protection Authorities publish guidelines for video conferencing systems (cont.)

From a technical point of view, notwithstanding the location of the service provider, each data flow should be secured by encryption in accordance with state of the art encryption mechanisms. In any case, if sensitive data is involved, the transmission should be encrypted end-to-end. Also, voice and video data should not be recorded, unless there is a legal basis. It should be noted that in Germany the unlawful recording of the spoken word, i.e. voice recording, is a criminal offence.

Moreover, the controller should ensure that data is only processed on the basis of and within the scope of the particular legal basis and that users are informed according to data protection rules. In addition, the (mutual) responsibilities of the service provider and the controller should be clarified and the service provider should be able to prove sufficient data security, e.g. by providing certificates, as well as provide technical and organizational measures.

Further recommendations of the German Data Protection Authorities include

- **Organizations should advise their employees and clients on how to act "data economically", e.g. only to use video conferencing when necessary or to allow the attendance without an active camera to protect the privacy of employees or client's homes.**
- **Organizations should also employ a data protection officer, determine rules regarding confidential topics that should not be discussed via video conferencing and give information on how to act when a violation, i.e. a data breach, is suspected.**

Germany

Court restricts right of access in case of disproportionate effort

On 6 February, 2020, the district court of Heidelberg decided that a right of access of the data subject does not exist if there is an imbalance between the effort in procurement of personal data and the data subject's interest to this information.

Despite of the seemingly explicit wording of Art. 15 GDPR, the scope of the right of access is still discussed controversially. In former judicial decisions the right of access was interpreted rather broadly in favor of the data subject. In the current case, the court denied the right of access by the data subject due to a disproportionate effort.

The plaintiff, a former member of the board, claimed access to all available personal data processed by his former employer, including copies of all the information. Alternatively, he claimed access to all information regarding his correspondence via e-mail over a period of more than one year, also including equivalent copies. Both claims were dismissed as unfounded.

Concerning the general request, to get access to all data processed including copies of such information, the court justified its rejection of the request by referencing recital 63 of the GDPR which states that controllers that process a large quantity of personal data may request that the data subject specifies the information or processing activities to which the request relates. The plaintiff clearly did not limit his claim to a certain area or category of information or processing activities but demanded all personal data relating to him that his former employer ever processed.

With regard to the alternative claim, to get access to e-mail correspondence over a period of more than one year, the court stated that although this claim was sufficiently determined, it failed due to a disproportionate effort for the former employer.

Germany

Court restricts right of access in case of disproportionate effort (cont.)

The court doubted that the former employer, i.e. the controller, still processed the data. In this regard, it is important that the controller had meanwhile become insolvent and all data had been handed over to a third party for backup purposes. According to the court, a controller is not obliged to give access to data processed in the past that is no longer at its disposal. This poses the key question whether the retrieval of the e-mails and the sighting and redaction of restricted data would involve a disproportionate effort for the controller. In order to decide this question, the court balanced the interests of both parties. It concluded that interests of the controller, i.e. the defendant, prevailed clearly.

The court considered that the relevant data would, as a first step, need to be obtained by the controller from the back-up. The cost of restoration alone would amount up to € 4,000. In addition, the court assumed that the e-mail correspondence comprised several thousands of e-mails, since the data subject had been a member of the board for at least one or one year and a half. The potential processing of the data would also tie up disproportionate resources of the controller. Further, the e-mails would have had to be reviewed and redacted to safeguard the legitimate interests of third parties before they could have been released to the data subject. The information interest of the data subject, however, could be classified lower than the one of the controller as the e-mails were already nine or ten years old, the data subject had not been working for the controller for nine years and the controller had meanwhile become insolvent.

This judgement is another step in the direction of clarifying the right of access. It can be helpful for companies to argue that they deny the right as the granting of the right of access according to Art. 15 GDPR would imply disproportionate effort in the retrieval of the data, in particular as it would tie up a lot of resources and incur high costs. It should, however, be noted that a decision of the European Court of Justice that would finally settle the question, does not yet exist and that the current case law varies tremendously.

Germany

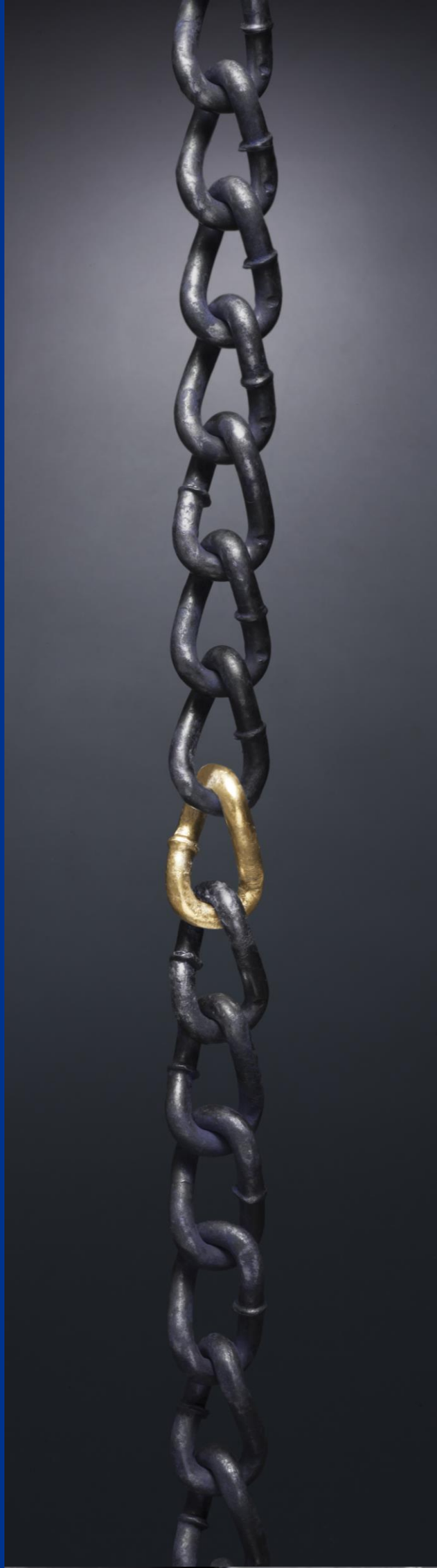
Data protection: ongoing infringement procedure against Germany

The EU Commission urges Germany to complete the transposition of the Data Protection Law Enforcement Directive.

The EU Commission accuses the Federal Republic of Germany of having failed to fully transpose the Data Protection Law Enforcement Directive and is therefore pressing ahead with infringement procedures.

The Directive protects citizens' fundamental right to data protection whenever criminal law enforcement authorities use personal data for law enforcement purposes. These rules aim to ensure that the personal data of victims, witnesses, and suspects of crimes are duly protected. The introduction of similar data protection standards across the EU shall facilitate the exchange of personal data for cross-border cooperation in the fight against crime and terrorism. Member States had until 6 May 2018 to transpose the Directive into their national laws. The Commission complains that five of the sixteen German federal states have not yet taken any measures to implement the Directive. The other eleven have already completed this task, though accompanied by controversial reforms of their police laws.

The Commission had already requested information on the transposition process from Germany on 25 July 2019. After further ten months, the Commission now opened the second stage in the infringement procedure on 14 May 2020 against Germany (and Slovenia) setting a time limit of four months for Germany to respond and take the relevant actions. Otherwise, the Commission can refer the case to the European Court of Justice of the EU.



Germany

If you have any questions, please let us know

Sebastian Hoegl, LL.M. (Wellington)
Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
M: + 49 761 76999-920
E: jshoegl@kpmg-law.com

Thorsten Jansen
Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
M: +49 221 271689-1364
E: thorstenjansen@kpmg-law.com

Maik Ringel
Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
M: +49 341 22572546
E: mringel@kpmg-law.com

Nikola A. F. Werry, LL.M. (UK)
Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
M: +49 69 951195-027
E: nwerry@kpmg-law.com

Hungary

A. The Hungarian DPA published its annual report for the year of 2019

B. Derogations from certain data protection provisions during the COVID-19 situation

C. Guideline regarding the coronavirus situation by the Hungarian DPA

Hungary

The Hungarian DPA published its annual report for the year of 2019

The Hungarian Data Protection Authority published its annual report for the year of 2019 at the end of March, 2020. The Authority reports on its year-round activity regarding the application of GDPR.

According to the statistical data of the report, more and more official procedures start at the data subjects' requests meaning that data subjects are getting increasingly aware of the importance of their personal data's protection.

The most typical requests for initiating the DPA's procedure were submitted to the DPA in relation to:

— Data processing conducted by employers

— Data processing conducted by claim management companies

— Camera surveillance

— Data processing by banks and insurers

— Processing of health data

— Data processing by insurers

— Data processing relating to assignment of claims

— Right of access to personal data

— Failure or rejection to perform data subject's rights.

Hungary

The Hungarian DPA published its annual report for the year of 2019 (cont.)

Data Protection incidents

In total **506 data protection incidents** were reported to the Hungarian Data Protection Authority in 2019.

The annual report shows that in most cases the incidents arose **due to the lack of security measures or inadequacy of existing ones. Therefore, according to the DPA, among others, the following key aspects are recommended to be considered in order to prevent data protection incidents:**

- **performing proper technical and organizational measures** i.e., Introduction of internal incident handling procedures, protection of the data carrier by technical measures which prevent unauthorized persons from having access to the data on the data carrier, even in the event of loss;
- **data security should also be ensured in case of paper-based data processing**;
- **guaranteeing security measures proportional** to the risk (e.g. documents containing health data should be posted as registered mail)

Hungary

Derogations from certain data protection provisions during the COVID-19 situation

The exercise of the data subject's rights laid down by the GDPR and the Hungarian Privacy Act **should be restricted** in relation to data processing conducted with the aim of preventing, better understanding, detecting, and avoiding the further spread of coronavirus cases (including the organization of the coordinated performance of the tasks of state organs), pursuant to Government Decree No. 179/2020. (V.4.) **as of 5 May until the end of the COVID-19 situation.**

The Government Decree has established a restriction on the rights of data subjects with regard to data processing concluded for the purposes defined above (e.g. prevention of the spread of coronavirus cases). Consequently, it appears that the rights of data subjects should continue to be ensured in the manner laid down by the GDPR and the Privacy Act with regard to data processing conducted for other purposes.

The rules shall also apply to data processing already in progress upon the entry into force of the Government Decree, as well as to related requests, notifications and procedures.

Hungary

Derogations from certain data protection provisions during the COVID-19 situation (cont.)

The most important measures introduced by the Government Decree

Suspension of measures to be taken upon an incoming request from a data subject

- With regard to the processing of data for the aforementioned purposes, all measures to be taken on the basis of the data subject's request shall be suspended until the end of the COVID-19 situation.
- The starting date of the time limits set for these measures shall be the day following the end of the COVID-19 situation.
- The data subject shall be informed immediately after the end of the COVID-19 situation, but not later than 90 days after receipt of the request.

Providing the right to prior notice by electronic means

The information to be provided in connection with the right to prior notice in the case of processing data for such purposes should be deemed to have been fulfilled if:

- general information published electronically on
- the purpose,
- the legal basis, and
- the scope of the processing

is available to the data subjects in clear and plain language.

The starting date of the time limit for procedures initiated upon complaints and the right to remedy

The starting date of the time limit set for proceedings initiated on the basis of a notification, request or statement of claim submitted in connection with the right to lodge a complaint with the Data Protection Authority or the right to an effective judicial remedy against a controller/processor or the Data Protection Authority shall be the day following the end of the period of the COVID-19 situation.

Hungary

Guideline regarding the coronavirus situation by the Hungarian DPA

With regard to the spread of the coronavirus, on March 10, 2020, the Hungarian Data Protection Authority issued a Guideline on processing data related to the coronavirus pandemic. We summarized the key aspects that should be taken into account in relation to data processing concluded by employers.

Key measures expected to be implemented by the employer

According to the Guideline, the introduction of a so-called pandemic/business continuity action plan is required. It is recommended to extend it to privacy controls to be taken based on the principle of privacy-by-design (e.g. development of preventive steps, building channels of communication, risk assessment).

A detailed data protection notification should also be made available to the employees, including the most important issues in relation to the coronavirus (e.g. symptoms, period of incubation) and who to turn to in the event of any questions or symptoms.

Furthermore, the DPA laid down that if an employee reports potential exposure to the employer or the employer deems that the suspicion of exposure can be established from the data provided by the employee, the employer is entitled to record the data concerned. In this case, the legal basis of the processing may be legitimate interest (GDPR Article 6 (1) f). In the case of the processing of sensitive data (e.g. data concerning health) the condition laid down by Article 9 (2) b) of the GDPR is applicable.

Hungary

If you have any questions, please let us know

dr. Bálint Tóásó MSc LL.M (Vienna)
Partner, Head of Legal Services
KPMG Legal Tóásó Law Firm
M: +36 30 663-6245
E: balint.toaso@kpmg.hu

dr. Fanni Markus
Associate
KPMG Legal Tóásó Law Firm
M: +36 70 333 1502
E: fanni.markus@kpmg.hu

Italy

A. Online journalism: the publication of entire investigative documents is forbidden

B. Urgency measure issued against a certified email service provider

Italy

Online journalism: the publication of entire investigative documents is forbidden

The Italian Data Protection Authority has forbidden to an online journal the further reproduction of a copy of an investigative document that was uploaded online in attachment to an article concerning the relevant ongoing investigations.

According to the Italian Data Protection Authority, the publication of the investigative document was in breach of both the applicable data protection and criminal procedure laws.

Focusing on the data protection related matters, the intervention of the Italian Data Protection Authority was triggered by several complaints filed by the professionals that were subject to the aforementioned investigation.

Such complaints were based on the fact that the amount of personal data of the professionals that have been disclosed to the general public (as contained in the investigative documents published by the online journal) were exceeding the disclosable amount of personal data pursuant to the correct application of the so-called "right to inform", whereas - by mean of the publication of the entire content of the investigative document - their names, surnames, emails address, personal address, personal phone number were published online.

40

Italy

Online journalism: the publication of entire investigative documents is forbidden (cont.)

The head editor of the online journal stated that such conduct should have to be considered admitted pursuant to the right to inform.

The Italian Data Protection Authority stated that the disclosure to the general public of the personal data of any person subject to formal investigations can be considered lawful under the right to inform provided that such disclosure of personal data concern a news (e.g. an investigation) of common and general interest and that the personal data effectively disclosed are limited to the ones essential for the correct understanding of the news.

Given the above, the Italian Data Protection Authority stated that the disclosure of the entire investigative document (containing names, surnames, addresses, phone numbers exc.) has to be considered as not covered by the right to inform, therefore it shall to be considered as in breach of the applicable data protection laws.

The Italian Data Protection Authority also stated that such disclosure has to be considered as in violation also of several articles of the Italian Code of Criminal Procedure.

Urgency measure issued against a certified email service provider

The Italian Data Protection Authority issued an urgency measure against one of the major Italian certified email service providers, concerning the IT security measures to be implemented in order to make their service - that are provided to more than 6mln corporations and professionals - compliant with the data protection laws.

During the second semester of 2019, the Italian Data Protection Authority carried out a specific inspection concerning the security measures adopted by the service provider concerning its certified email services.

The results of such inspection were as follows: after one year after the activation of the certified email service, over 580,000 single users were utilizing the first password, as initially chosen either from the service provider or its partners that were re-selling the service, without the provision of the mandatory modification of the initial password.

In addition to that, the inspection carried out by the Italian Data Protection Authority highlighted other vulnerabilities, such as:

— the technical passwords of the management of several services were reported in the tracking log of the relevant operations, thus enhancing the risk of non-controlled access both from internal non-authorized persons and hackers;

— several users were granted with high-level access privileges (so-called "Super-Admin") that allowed such users access to the log concerning the email exchanged between 6 mln email addresses, thus violating the basic security principles of providing different individual passwords to different users accessing the same repositories.

Given the above, the Italian Data Protection Authority has imposed on the service provider the adoption of the following measures:

— mandatory modification of the initial password assigned to each user successively to its first access to its email box;

— re-definition of the log system, thus providing that such log would contain only the data strictly required for security purposes;

— modification of the email logs' consultation and export modalities.

It is worth noting that the Italian Data Protection Authority has issued the urgency measure immediately after the inspection was performed, but such measure has been published only after the Company has performed the mandatory modifications to its systems and security procedures, in order to avoid the risk that any third party would take advantage of the vulnerabilities identified during the inspection.

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

Poland

A. First judgement regarding the penalty for failure to comply with GDPR

B. The electronic form of the authorisation shall comply with the requirements of the "written authorisation"

C. If the employer runs the Company's Social Benefits Fund, it is also subject to GDPR.

D. Judgment confirming the decision of the Polish authority

E. Penalty for processing of biometric data

F. Polish authority's statement on data proceeding due to COVID-19

G. Data breach proceedings

Poland

First judgment regarding the penalty for failure to comply with GDPR

A judgment of the Voivodship Administrative Court in Warsaw of 11 December 2019 stated that the entity obtaining personal data of entrepreneurs from public registers in order to provide commercial services is obliged to fulfil the information obligation directly to these persons. Furthermore, in the Court's opinion, a possible high cost of sending this information by traditional mail is not a basis for exemption from the information obligation.

The Polish authority has penalized the Company (entity delivering credit and market information) in connection with the violation of the obligation to provide information (Article 14 paragraphs 1-3 of GDPR), consisting of the failure to provide information contained in Article 14 paragraphs 1 and 2 of GDPR to all natural persons whose personal data is processed by the Company, conducting currently or in the past sole proprietorship and natural persons who suspended their activities.

At the same time, the Court, due to certain procedural irregularities, set aside the decision of the Polish authority in the part concerning the order to fulfil the information obligation towards natural persons conducting business activity in the past. The Court also repealed the financial penalty, because it considered that it is disproportionate in the given situation, since it referred to a lack of information also towards persons who had ceased business activity.

A new amount of the penalty shall be re-imposed by the Polish authority.

Poland

The electronic form of the authorisation shall comply with the requirements of the 'written authorisation'

The granting of authorisations in electronic form should be considered a performance of the obligation to grant authorisations in writing.

In light of the principle of accountability, any form, including electronic form, which allows to document the fulfilment of obligations in order to prove the compliance with the regulations, and in this case the fulfilment of the obligation processing data under the authority of the controller or processor, should be considered correct.

The approach to the written form set out in Article 30(3) of GDPR is also in favour of adopting such a position. According to this provision, the register of processing activities and the register of categories of processing activities shall be in writing, including electronic form. As indicated in the manual on this obligation (Guidelines and explanations concerning the obligation to register processing activities and categories of processing activities specified in Article 30(1) and (2) of GDPR), registers should be kept in written form (Article 30(3)) and therefore they may be kept both in paper and electronic form.

Poland

If the employer runs the Company's Social Benefits Fund, it is also subject to GDPR

In order to grant an employee a benefit from the Company's Social Benefit Fund, the employer must know and assess the life and financial situation of the employee and the members of his family with whom he shares a household. In order to meet these needs, he must therefore process the personal data of these persons, but only those data which are necessary for the purpose of which he obtained them. The employer is also obliged to review these data at least once a year.

Granting of benefits, as well as their amount, depends on the fulfilment of certain social criteria by the claimant. Company's Social Benefits Fund Act obliges an employer to make the granting of the benefit conditional on the life, family and financial situation of the person entitled to benefit from the Fund.

This means that the employer must know and assess the life and financial situation of all members of the employee's family with whom he/she runs a joint household. Therefore, in order to meet these needs, the employer must process personal data of the employee and his/her family members. However, the processing of these data must not lead to the collection of data to a greater extent than is necessary for the purpose of which they are collected. The Act specifies that the employee submits these data to the employer in the form of a declaration. However, confirmation of the data contained therein may take place, among others, on the basis of statements and certificates of life situation. The Act allows the employer only to view them but does not give the right to keep copies thereof.

The provisions of the Act assume that an employer, under the Fund, processes personal data for the period necessary to grant a discounted service and provision or subsidy from this source and to determine its amount, as well as for the period necessary to assert rights or claims (e.g. tax liabilities become time-barred after five years).

Poland

Judgment confirming the decision of the Polish authority

The Voivodship Administrative Court in Warsaw confirmed the legitimacy of the penalty imposed on the Lower Silesian Football Association.

The Court upheld the decision of the Polish authority imposing an administrative fine of PLN 55,750.50. The Lower Silesian Football Association published in the network personal data of judges who were granted judicial licenses. Their names, exact addresses and PESEL numbers were given. The Polish authority decided that there is no legal basis for making such a wide range of judges' data available on the Internet. The Court shared the view of the Polish authority that the processing of personal data should be guided by the principle of minimisation (Article 5(1)(c) of GDPR).

Moreover, the Court supported the argument that publishing such data as name, surname, address and PESEL may lead to far-reaching negative consequences for the data subjects. By making such data available on the Internet, the controller posed a potential risk of their unlawful use, e.g. to impersonate these persons in order to make financial commitments.

The Court did not share the applicant's argument that non-professional data processors are exempt from the application of data protection legislation.

Poland

Penalty for the non-compliance of processing of biometric data

The Polish authority imposed a fine of PLN 20,000 in connection with an infringement consisting of processing children's biometric data while using the school canteen.

In the opinion of the Polish authority the school processed special categories of data (biometric data) of 680 children without a legal basis, while being able to use other forms of student identification.

For this violation an administrative fine was imposed on a primary school. Moreover, the Polish authority ordered the school to delete personal data processed in digital form of information about characteristic fingerprint points of the children's fingers and to stop further collection of personal data.

The Polish authority established that the school uses a biometric reader at the entrance to the school canteen, which identifies children in order to verify payment of the meal fee.

The proceedings showed that the school collects this data and processes it on the basis of written consent of parents or legal guardians. This solution has been applied since 1 April 2015. In the current school year 2019/2020, 680 students use the biometric reader and 4 students use an alternative identification system.

In the opinion of the Polish authority, the processing of biometric data is not necessary to achieve the purpose of identifying a child's entitlement to collect lunch. The school can carry out the identification by other means which do not interfere so much with the child's privacy.

As soon as all students with biometric identifications enter the canteen, single students without biometric identifications will be allowed in. According to the Polish authority, such rules introduce unequal treatment of students and unjustified differentiation because they clearly promote students with biometric identifications.

The biometric system identifies attributes which do not change and often - as in the case of dactyloscopic data – are impossible to change. Due to the uniqueness and permanence of biometric data, which reflects in their unchangeability over time, the use of biometric data should be done with caution and consideration. Biometric data are unique in the light of fundamental human rights and freedoms and therefore require exceptional protection.

Polish authority's statement on data proceedings due to COVID-19

The Polish authority highlights that the issues related to COVID-19 are regulated by the specific legal provisions, including in particular the so-called "COVID-19 Special Act". The provisions on personal data protection cannot be considered as an obstacle to conducting the activities with regard to fighting the virus.

The legal provisions of the COVID-19 Special Act do not conflict with the principles of data processing and do not violate GDPR. The Act provides tools for undertaking specific activities by the employers that result both from the recommendations of the Chief Sanitary Inspector and the Prime Minister.

Article 17 of the COVID-19 Special Act sets forth that the Chief Sanitary Inspector or the voivodeship sanitary inspector acting on its behalf can issue to employers, among others, **decisions imposing an obligation to undertake specific prevention** or inspection actions and cooperation with other public administration authorities and State Sanitary Inspection authorities. As part of the activities undertaken by the employers, they in particular have to stay abreast of the communications by the State Sanitary Inspection.

The Prime Minister at the request of the voivode, after having informed the minister of economy, shall have the right to issue **instructions to the entrepreneurs** in connection with preventing COVID-19.

These instructions, issued in the form of an administrative decision, shall be implemented immediately upon its delivery or announcement and do not require statement of reasons.

These legal provisions correspond to GDPR provisions which also provide for the situations related to the protection of health and preventing spread of infectious diseases (Art. 9(2)(i) and Art. 6(1)(d). Pursuant to recital 46 of GDPR the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject, for example where the processing is necessary for humanitarian purposes, including monitoring epidemics and their spread.

In the opinion of the Polish authority, the regulations on the protection of personal data do not object to the processing of the data of employees and guests in the scope of e.g. temperature measurement or implementation of the questionnaire with disease symptoms. Article 9(2)(i) of GDPR indicates that special categories of (health-related) data may be processed when necessary for reasons of public interest in the field of public health, such as protection against serious cross-border health threats, if this is provided for by law provision. And the above mentioned article 17 of the COVID-19 Special Act could potentially be regarded as such particular provision (although it is not entirely undisputable).

Poland

Data breach proceedings

During the last few months the Polish authority commenced proceedings on data breach and leakage. The most important of them are:

1. Proceedings against the Warsaw University of Life Sciences

Following an inspection performed at the Warsaw University of Life Sciences (SGGW) in connection with the data protection breach, the Polish authority initiated administrative proceedings. A stolen laptop, containing the data of candidates for studies at SGGW, belonged to a staff member of the university. The inspection showed clear dysfunctions in the data protection system at the university, from both a technical and an organisational point of view. It was found that the security policy adopted at the university was not updated and reviewed. In the course of the inspection it was established that the controller did not duly review the processing of personal data of candidates for studies. Therefore, it did not have sufficient knowledge of the risks involved in that processing and did not take appropriate action under, inter alia, Article 25(1) or 32(1)(b) and (d) of GDPR. The inspection activities have also revealed irregularities in the performance of the function of the data protection officer who, inter alia, did not perform his/her tasks in accordance with Article 39(2) of GDPR, i.e. having due regard for the risk associated with processing operations.

2. MoneyMan data leakage

The Polish authority received a personal data breach notification from an entity maintaining a lending platform MoneyMan.pl. The case is currently being analysed by the Polish authority, and first activities have been undertaken aimed at explaining the exact circumstances of the breach. The controller informed the Polish authority that it has communicated the breach to the data subjects.

Data breach proceedings (cont.)

3. Fine imposed for preventing the Polish authority from performing an inspection

The Polish authority imposed a fine of PLN 20,000 upon a company from the telemarketing sector, for making it impossible to perform an inspection. Additionally, the company's owner is subject to criminal liability for this. The Polish authority concluded that the company in no way wished to cooperate with the Polish authority. On two consecutive days of the planned inspection activities, the company made it impossible to carry out the inspection twice. Furthermore, on the date on which the inspectors attempted to conduct inspection at the company, its authorities decided to liquidate that entity.

In the opinion of the Polish authority, this company infringed the provisions of GDPR referring to cooperation with the supervisory authority and enabling it access to all personal data and any information. In connection with a suspicion that the President of the company has committed an offence, referred to in Article 108 of the Personal Data Protection Act of 10 May 2018, the Polish authority notified the District Public Prosecutor's Office thereof. According to the abovementioned provision, the prevention or hindering of conducting an inspection of compliance with the personal data protection provisions shall be subject to a fine, restriction of personal liberty or imprisonment for up to two years. The Public Prosecutor's Office has already lodged an indictment against the President of the Company to the court.

Poland

If you have any questions, please let us know

Magdalena Bęza
of Counsel
D.Dobkowski sp. k.
M: +48603988938
E: @mbeza@kpmg.pl

Natalia Kotłowska
Senior Associate
D.Dobkowski sp. k.
M: +48661111579
E: @nkotlowska@kpmg.pl

Romania

A. Processing health data in the context of COVID-19

B. Telecommunications provider fined for non-compliance with the GDPR

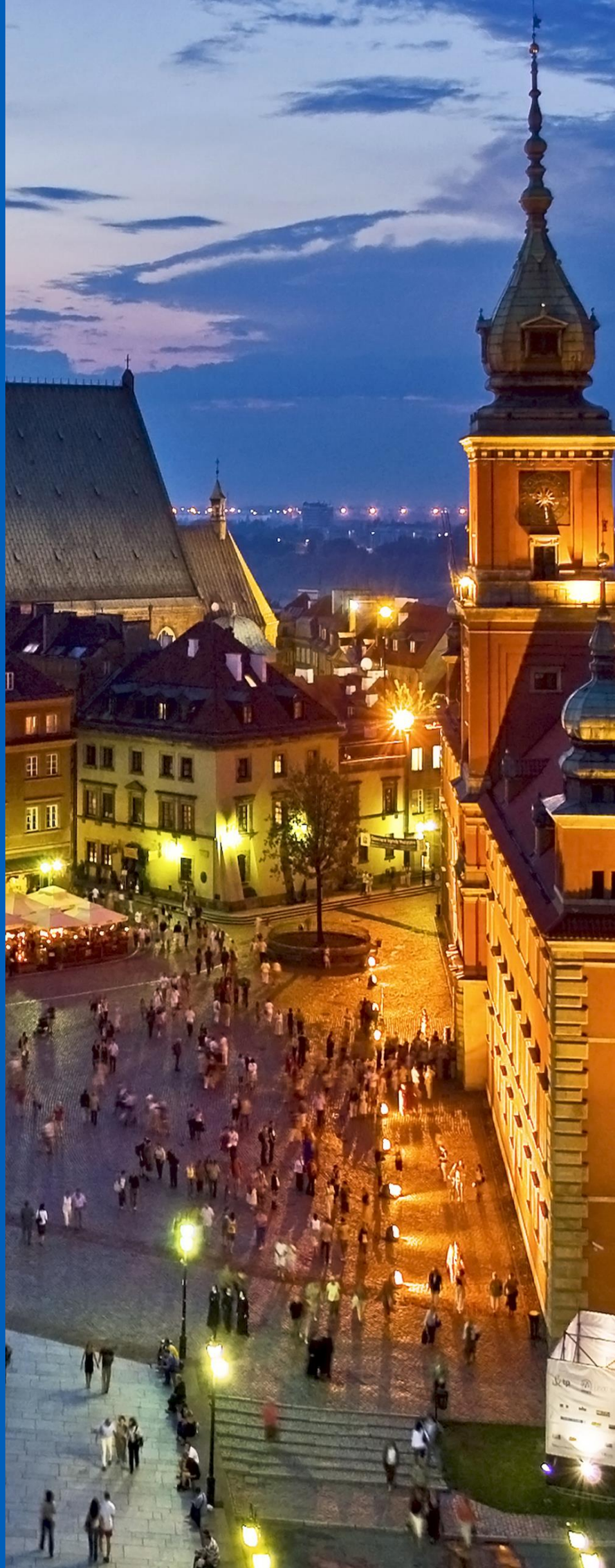
C. NGO fined for non-compliance with the GDPR

D. Electricity provider fined for non-compliance with the GDPR

E. Telecommunications provider fined for non-compliance with the Romanian ePrivacy Law

F. Online retail company fined for non-compliance with the GDPR

G. Banking institution fined for non-compliance with the GDPR



Romania

Processing health data in the context of COVID-19

On 18 March 2020, the Romanian Data Protection Authority published a recommendation concerning the processing of health data in the context of COVID-19.

The Data Protection Authority detailed that the processing of special categories of data can be made in accordance with the GDPR, provided that one of the following conditions is met:

— the data subject has given his explicit consent to the processing; or

— the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law; or

— processing is necessary for the purposes of preventive or occupational medicine; or

— processing is necessary for reasons of public interest in the area of public health.

Also, personal data other than those of special categories may be processed in compliance with Article 6 of the GDPR.

With regard to the obligation to inform the data subjects, the controllers should make sure that the information is provided in a concise, transparent, intelligible and easily accessible form, while using clear and simple language.

The controllers should ensure the security of processing and should implement technical and organizational measures to ensure they are able to demonstrate that processing is carried out in accordance with the GDPR.

Romania

Telecommunications provider fined for non-compliance with the GDPR

The Romanian Data Protection Authority fined a major telecommunications provider EUR 3,000 for non-compliance with the GDPR.

On 18 March 2020, the Data Protection Authority announced that it has fined a major telecommunications provider EUR 3,000 for non-compliance with the GDPR. The controller was sanctioned because it mistakenly processed personal data of a natural person in order to solve his complaint, by transmitting the controller's response to an incorrect e-mail address of another person, breaching thus the processing principles provided by the GDPR.

The additional corrective measure applied in this case provided the controller's obligation to ensure compliance with the GDPR of the operations for the collection and subsequent processing of personal data, by implementing efficient methods of respecting the accuracy of the data (e.g. e-mail addresses), including in the case of data collection. In this respect, the controller had to put in place adequate and efficient security measures from a technical and organizational point of view, including through regular training of persons that process data under the authority of the controller.

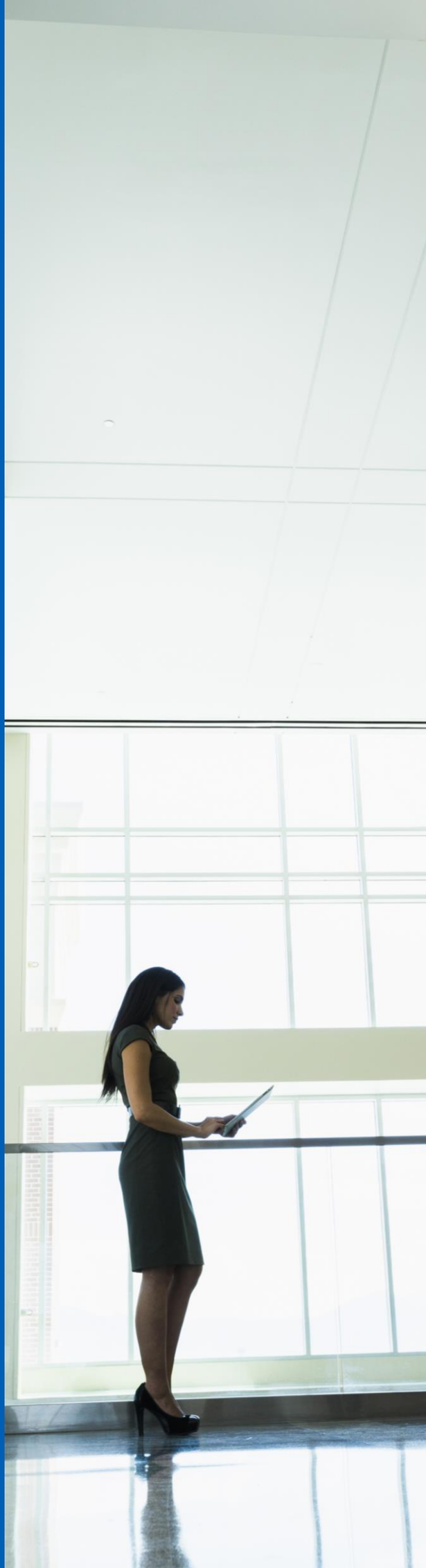
Romania

NGO fined for non-compliance with the GDPR

The Romanian Data Protection Authority fined an NGO active in the health domain EUR 2,000 for GDPR non-compliance.

On 25 March 2020, the Data Protection Authority announced that it had completed an investigation concerning the compliance of an NGO with the GDPR. The controller did not transmit the information requested by the Data Protection Authority, thus infringing the rules of the GDPR and was fined EUR 2,000.

The Data Protection Authority was notified that the association has disclosed personal data without the consent of the data subject. As the Data Protection Authority tried repeatedly to contact the association for more information without any result and finally after managing to contact the president of the association that recommended to the authority to send the request by e-mail, the association still did not respond. In this situation, a corrective measure and a fine was imposed on the controller.



Romania

Electricity provider fined for non-compliance with the GDPR

The Romanian Data Protection Authority fined an electricity provider EUR 3,000 for non-compliance with the GDPR.

On 25 March 2020, the Data Protection Authority announced that a major electricity provider violated the provisions of the GDPR, concerning the security of processing personal data. A fine of EUR 3,000 was imposed on the controller.

The violation of the security and confidentiality of the personal data was caused by the fact that the controller sent to the e-mail address of a client (natural person), personal data (name and surname, address, e-mail address, client code) of another client. The controller was sanctioned because it did not implement adequate technical and organizational measures in order to ensure a level of security corresponding to the risk of the processing generated especially, accidentally or illegally, by the unauthorized disclosure or the unauthorized access to personal data.

Romania

Telecommunications provider fined for non-compliance with the Romanian ePrivacy Law

On 25 March 2020, the Romanian Data Protection Authority announced that it has issued 2 fines to a major telecommunications provider in total amount of EUR 4,140 for non-compliance with the provisions of the Law no. 506/2004 regarding the security and confidentiality of personal data GDPR.

A petitioner claimed that she requested an offer by telephone, through the website of the controller and that, subsequently, she received on her e-mail address, a contract concluded by the controller with another person (the petitioner suspecting that her personal data may have been disclosed to this person).

As a result of the investigation conducted at the controller, the Data Protection Authority found that the first violation of the law consisted in non-compliance with the provisions according to which the provider of an electronic communications service has the obligation to take appropriate technical and organizational measures in order to ensure the security of the processing of personal data. Also, the measures must ensure a proportional level of security in relationship with the existing risk, taking into account the last-minute technical possibilities and the costs of implementing these measures.

The measures should comply with at least the following conditions:

— to guarantee that personal data can only be accessed by authorized persons, for the purposes authorized by law;

— to protect personal data stored or transmitted against accidental or unlawful destruction, against accidental loss or damage and against unlawful storage, processing, access or disclosure;

— to ensure the implementation of the security policy developed by the provider regarding the processing of personal data

The second infringement consisted in the failure to notify the security breach, without delay, to the Data Protection Authority.

Romania

Online retail company fined for non-compliance with the GDPR

On 25 March 2020, the Romanian Data Protection Authority announced that it has fined a major online retail company EUR 3,000 for non-compliance with the GDPR.

The sanction was applied because at the end of 2019 the controller sent a commercial message to a natural person, although at the beginning of 2019 it had confirmed to that person that the unsubscription from commercial communications was completed.

The controller was also obliged to cease sending commercial messages on the data's subject e-mail address.

Romania

Banking institution fined for non-compliance with the GDPR

On 5 May 2020, the Romanian Data Protection Authority announced that it has fined a banking institution EUR 5,000 for non-compliance with the GDPR.

The banking institution has not implemented adequate technical and organizational measures to ensure a level of security appropriate to the risk of processing. Thus, the Data Protection Authority found that an employee of the bank has used his personal phone in order to collect copies of ID cards of individual clients and has forwarded the copies to other bank employees using a mobile messaging app, in violation of the internal working procedure.

Romania

If you have any questions, please let us know

Cristiana Fernbach
Partner, KPMG Legal
KPMG Legal acts in Romania through Toncescu si Asociatii
T: +40 372 377 800
E: cfernbach@kpmg.com

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

Flavius Florea
Senior Manager
KPMG in Romania
T: +40372377800
E: fflorea@kpmg.com

Spain

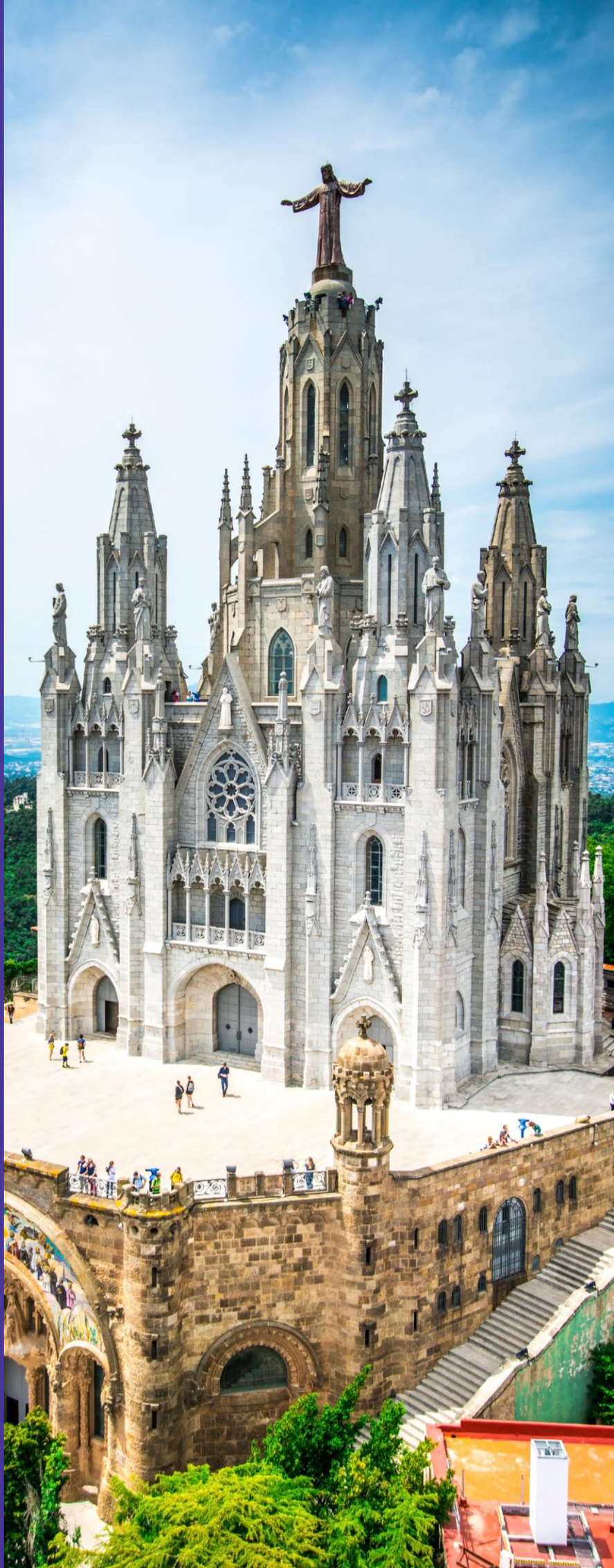
A. **The Spanish Data Protection Commissioner publishes some guidance notes regarding temperature controls at shops, workplaces and other establishments**

B. **The Spanish Data Protection Commissioner publishes a report on data processing in relation to COVID-19**

C. **The Spanish Data Protection Commissioner publishes a study analyzing different technologies to fight the Coronavirus and its privacy risks**

D. **The Spanish Data Protection Commissioner publishes a data protection impact assessment template**

E. **The Spanish Data Protection Commissioner publishes its 2019 report, the first covering a full year since the implementation of the GDPR**



Spain

The Spanish Data Protection Commissioner publishes some guidance notes regarding temperature controls at shops, workplaces and other establishments

The limitation of economic and social activity is driving the implementation of measures aimed at preventing new COVID - 19 infections. These measures include temperature control to allow people access to work centers, shops, educational centers or other types of establishments.

This data processing represents a significant intrusion in the rights of the data subjects. On the one hand, because it affects special categories of personal data and because, on the basis of this information, it is assumed that a person does or does not suffer from a specific disease, in this case, the Coronavirus.

In addition, the consequences of an access denial to a certain place as a result of temperature control can have a significant impact on the person concerned.

The Spanish Data Protection Commissioner (AEPD) states that the implementation of these measures and the subsequent data processing requires the competent health authority (the Ministry of Health) to decide on their necessity and adequacy for the purpose of contributing effectively to the prevention of the spread of the disease, as well as to regulate the specific limits and guarantees for the processing of personal data.

This data processing must comply with the principle of lawfulness (Articles 6.1 and 9.2 GDPR). The AEPD therefore rules out consent and legitimate interest as adequate grounds for lawfulness, and suggests that in the working environment, such processing could be covered by the legal obligation of employers to ensure the safety and health of employees.

In other areas, it could be argued that the general interests for public health require protection. However, this possibility would also require, as established in Article 9.2.i GDPR, a regulatory support through laws establishing this interest and providing adequate and specific guarantees to protect the rights and freedoms of the data subjects.

There have been conflicting views on this topic. Where the temperature control is manually operated, there are solid grounds for defense that the privacy regulations do not apply, and so have been stated by other control authorities and some Spanish authors.

Spain

The Spanish Data Protection Commissioner publishes a report on data processing in relation to COVID-19

The AEPD clarifies that data processing in the context of the pandemic, including health data, is legitimate under certain circumstances and that processing for pandemic containment purposes should be coordinated by health authorities.

The analysis carried out by the AEPD can be summarized in two points:

— The processing of personal data, including health data, may be covered by the following legal grounds: (i) mission carried out in the public interest (Art. 6.1.e), vital interests of the data subjects or other natural persons (Art. 6.1.d)

— Processing of special categories of data by data controllers (including employers) shall be feasible, but with limitations, in accordance with Article 9 of GDPR

Concerning employers, the AEPD distinguishes between:

— processing of data obtained from communications made by employees, whose duty is to report any situation involving risks to the safety and health of employees, and

— processing operations carried out in order to safeguard the vital interests of natural persons or essential public health interests.

For the former, the employer shall determine which processing operations are necessary to protect employees (always applying the principle of data minimization), for the latter, the data controllers shall follow the indications/instructions of the health authorities in any case.

Thereafter, the AEPD published a document including FAQs about the processing activities that can be carried out in relation to the COVID-19 prevention, which represents a relevant change in criteria with respect to what the previous report proposed.

Specifically, the AEPD establishes that companies can:

— carry out temperature controls on their employees, provided that they process the data exclusively for the specific purpose of containing the spread of the Coronavirus and provided that the data are kept for no longer than as necessary to carry out this purpose; and

— ask questions from their employees provided they merely inquire about the existence of symptoms, or whether the employee has been diagnosed as infected, or subject to quarantine, because of the Coronavirus.

Spain

The Spanish Data Protection Commissioner publishes a study analyzing different technologies to fight the Coronavirus and its risks to privacy

The AEPD examines the relationship between the potential benefits of pandemic control and the privacy risks involved in using these technologies

The AEPD stated that the state of emergency declared in Spain cannot imply a suspension of the fundamental right to the protection of personal data. But, at the same time, the data protection regulations cannot be used to hinder or limit the effectiveness of the measures adopted by the competent authorities, especially the health authorities, in the fight against the pandemic. To this end, the AEPD is collaborating with the competent authorities by providing them with criteria that allow to make technology fighting the COVID-19 compatible with privacy.

The report provides a preliminary analysis of seven systems: geolocation collected by telecom operators; geolocation in social networks; apps, websites and chatbots for self-testing or appointment; voluntary infection information apps; Bluetooth contact tracking apps; immunity passports and infrared cameras.

The document points out that the success of these types of solutions is based on factors that do not depend solely on technology. There are other determining factors for their effectiveness, such as the involvement of a large number of users, the guarantee of a responsible approach or the access to reliable periodical health checks in order to be able to update the information collected by these systems.

The Spanish Data Protection Commissioner publishes a data protection impact assessment template

The AEPD publishes a DPIA template to help companies in the process of carrying out data protection impact assessments.

The document compiles the aspects that must be considered by the private sector to produce an Impact Assessment Report.

The GDPR provides that data controllers should assess the impact of the data processing operations they carry out where these are likely to result in a high risk to the rights and freedoms of individuals.

To assist data controllers in carrying out this obligation, the AEPD has published a template report compiling all the aspects to be taken into account in order to draft an impact assessment report, including a description of the processing operation, its purpose, the legal grounds for the processing, the reasons for which a DPIA should be carried out, risk reduction measures, an action plan and a section on conclusions and recommendations.

The AEPD also states that in those cases in which it is not mandatory to carry out an impact assessment, the opportunity of carrying out this analysis for other purposes may be assessed, such as studying in depth how the data are being processed; improving the global management of the processes of an organization; generating knowledge and a culture of data protection, or performing accountability.

This template is a complement to the AEPD's initiatives to provide guidelines and resources to data controllers, such as the Guide for Risk Analysis and the Practical Guide for Data Protection Impact Assessments.

Spain

The Spanish Data Protection Commissioner publishes its 2019 report, the first covering a full year since the implementation of the GDPR

This document includes the activities carried out by the AEPD, the management figures, the most important trends, the most relevant decisions and procedures of the year, and an analysis of the present and future challenges.

Regarding complaints, 11,590 have been filed during 2019. The most frequent complaints made by citizens in 2019 refer to Internet services (13%), video surveillance (12%), undue insertion in debt files (12%) and debt claims and advertising (except spam) (9%).

Regarding sanctioning resolutions, 338 were issued, of which only 112 imposed a fine, with the total collected amounting to EUR 6,295,923. This represents a decrease in both the number of resolutions and sanctions from the previous year due mainly to three factors: (i) there are many complaints that can be resolved in previous stages, particularly in the transfer of claims to the DPO (ii) in the case of a minor infringement or when the fine constitutes a disproportionate burden for a natural person, a warning can be imposed instead of a fine (iii) since 25 May the AEPD goes beyond specific complaints to carry out major analysis of the data processing systems of the data controller. These investigations are very complex and take longer than an ordinary complaint, and therefore take longer to resolve.

Another novelty to be highlighted is the increase in cross-border cases, where the AEPD has been involved in 21 new cases as the leading authority and in 565 as the supervisory authority concerned.

Finally, 1,459 security incidents have been reported in 2019, almost tripling the number received the previous year (547). At this point, it is necessary to mention that only 79 have been referred to the Inspection as they required an in-depth investigation.

Spain

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

Claire Murphy
Lawyer
KPMG Spain
T: +34 91 4563400
E: clairemurphy3@kpmg.es

Turkey

A. Public announcements regarding protection of personal data during COVID-19 outbreak

B. Binding corporate rules

C. Data transfer commitments

D. Data breaches

Public announcements regarding protection of personal data during COVID-19 outbreak

The Personal Data Protection Board, Turkish DPA published various public announcements during the COVID-19 pandemic to guide the data controllers intaking the necessary measures to protect personal data during the outbreak.

Public Announcement Regarding the Legal Periods During COVID-19

First, the Turkish DPA announced that data controllers should continue to respect the periods stated by the Law on Personal Data Protection,, the KVKK and other legislation for submission of complaints, notices and data breach notifications to the Turkish DPA.

Later on, considering the extraordinary conditions that the data controllers are encountering, the Turkish DPA announced that they would take into consideration the extraordinary circumstances while evaluating the periods that data controllers were obliged to comply with.

Public announcement on distance learning platforms

Among the measures taken in order to protect the health, safety and security of both students and lecturers, schools have been shut down since March 2020. However, the lectures continue on distance learning platforms. The Turkish DPA has observed that personal data such as names and surnames of the students, as well as some special categories of personal data that can be evaluated within the scope of biometric data such as voice and image are processed, in such distant learning platforms.

The Turkish DPA reinforced that the processing of these personal data should comply with respective articles, which specifies the conditions for the processing of both personal and special categories of personal data. Furthermore, if these distance learning platforms use cloud systems with their data centers located abroad, then data controllers should adhere to the conditions of transferring personal data abroad under the KVKK and the related legislation.

Public announcement regarding the processing of location data and tracking mobility of individuals to combat COVID-19

As the COVID-19 virus spread and increased worldwide, the measures taken by the governments for protection from the virus also changed accordingly. In addition to classical measures such as quarantine application, social distance, and isolation, 21st-century technology systems that measure the distance and mobility of people based on the location data are now on the agenda. Hence, in Turkey, the Ministry of Health recently implemented the "Pandemic Insulation Tracking Project".

Provisions of KVKK do not apply in cases where personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorized and assigned by law to maintain national defense, national security, public security, and order or economic security.

Public announcements regarding protection of personal data during COVID-19 outbreak (cont.)

Accordingly, in the event of an epidemic, data processing activities to be carried out by competent public institutions and organizations to ensure isolation of people who have been diagnosed with the disease, to identify crowded areas by processing location data of the general population and to develop measures in these areas are deemed to fall in the scope of KVKK.

Public announcement regarding the protection of personal data during the fight against COVID-19

During the COVID-19 health crisis, governments inevitably process personal data in order to take crucial and necessary steps to prevent the outbreak. However, during this period, the Turkish DPA announced that data controllers must still act in accordance with the KVKK and other legislation. General principles on the protection of personal data must be at the core of all personal data processing activities, and all personal data processing activities must be carried out in accordance with the principles of lawfulness, privacy, transparency, and data minimization.

The Turkish DPA also answered frequently asked questions regarding personal data processing during the outbreak:

— Relevant health institutions will be able to send informative messages about public health to people via communication tools such as e-mail and SMS without obtaining the explicit consent of those concerned.

— Employers should not disclose the identity of an infected employee to other employees/colleagues unless it is necessary to disclose the employee's name to take the required protective measures for COVID-19. In such cases, the employee should be informed beforehand that his/her name will be disclosed.

— Employers may request information from employees and visitors regarding their travel histories and health conditions provided that the nature of the request has a strong rationale based on necessity and proportionality, and for risk management purposes, then the request will not be against the KVKK.

— During the outbreak, some workplaces switched their working system to "home office". KVKK will not be an obstacle to such types of remote working. However, institutions and organizations that switch to the home office must take the necessary administrative and technical measures to ensure personal data security.

— According to the KVKK, employers are allowed to share personal data of individuals infected with contagious diseases with relevant authorities.

Binding corporate rules

Turkish DPA regulated the binding corporate rules and recognized it as a method to transfer personal data abroad.

Previously published personal data transfer commitments generally facilitate the bilateral transfers to be made between the companies. However, they may fall behind in providing a practical implementation concerning the data transfers to be made between the multinational corporation communities. For this reason, the Turkish DPA has determined "Binding Corporate Rules" as another method to be used in the cross-border data transfers to be made between these corporate companies.

Data transfer commitments

The Turkish DPA published an announcement for commitments to be prepared for the transfer of personal data abroad.

The Turkish DPA has not yet published the list of countries that will be considered safe within the scope of the transfer of personal data abroad. For this reason, transferring of personal data abroad upon the permission of the Turkish DPA has been considered and allowed with certain commitments to be undertaken.

According to the relationship between the parties of the transfer and the nature of the recipient, the appropriate letter from the "Transfer from Data Controller to Data Controller" or "Transfer from Data Controller to Data Processor" commitments must be used.

The Turkish DPA listed the points to be considered while preparing the commitments in three sections in the appendix of the announcement.

Data breaches

Data breach notifications published by the Turkish DPA

The Turkish DPA has published four more data breach notifications on its official website since the previous newsletter. These notifications include data controllers such as banks, insurance companies, as well as various retail companies. One of the most recent notifications published on the official website is related to a data breach that occurred in one of the most popular cosmetic store chains;

The breach occurred between 04.04.2020 and 06.03.2020 and was detected on 06.03.2020. On 06.03.2020, an e-mail was received from an unidentified person about the obtainment of the e-mail addresses/passwords of the Web Site members of the Company.

More than one entry attempts were made with the e-mail addresses/passwords obtained by the sources out of the Company, and after every unsuccessful attempt, another e-mail/password attempt was made. Hence, passwords of 2092 web site users were verified.

Personal data categories affected by the breach are stated as identity, contact, and transaction data of 2092 customers have been affected by the breach.

If you have any questions, please let us know

Onur Küçük
Partner, Lawyer
KP Law
M: +902123166000 / 6021
E: onurkucuk@kphukuk.com

UK

A. Two years of the GDPR in the UK

B. ICO COVID-19 Response

C. ICO looks to the future

D. Contact tracing apps

E. Brexit

United Kingdom

Two years of the GDPR in the UK

Two years ago when the General Data Protection Regulation (GDPR) came into effect the threat of huge fines into the millions was very much at the forefront of people's minds as they finalised (or quietly continued to develop), and embedded GDPR compliance programmes for their organisations.

The ICO has conducted numerous investigations and taken enforcement action, consulted on revised guidance and codes of practice on such matters as marketing and data-sharing, whilst also tackling developing and complex issues such as artificial intelligence, facial recognition, Adtech, Brexit and of course the issues arising from the COVID-19 pandemic.

The lack of huge multi-million pound fines to date is due partly to timing, as many of the breaches under consideration occurred under the old data protection regime. However, even then the ICO has shown its teeth on occasion by fining up to the maximum permitted under that legislation (£500,000). They have also demonstrated that they intend to use the powers that they have to fine under the GDPR, by publishing notices of intention to impose fines of multi-million pounds and fines are not the only method of enforcement available to the ICO. They can also serve enforcement notices, requiring organisations to take expensive action or to cease processing all together, which could have dire economic consequences.

Whilst the ICO is currently demonstrating its pragmatic approach during the COVID-19 pandemic, it must be remembered that, for post Brexit (in particular in relation to data flows to the UK from the European Union ("EU")), the UK is looking for an assessment of "adequacy" of its data protection laws from the EU. The ICO must therefore be seen to be maintaining the standards imposed by the EU GDPR and reiterates that it will take robust action, where it deems necessary.

ICO COVID-19 Response

The ICO was quick to release early guidance to address concerns arising during the pandemic:

—Approach to Enforcement during this period:

The ICO acknowledges that organisations may now have less resource available and has pragmatically advised that they won't penalise organisations that they know need to prioritise other areas or otherwise adapt. They can't extend statutory timescales, but have said they will raise awareness that there may be understandable delays to responses to information rights requests during the pandemic; not a change to the law but a clear indication that the ICO is sympathetic to the challenges that businesses face at this extraordinary time.

—Data Protection compliance during the pandemic:

Businesses are having to adapt very quickly to the crisis to sustain themselves (in many cases redefining their business models), whilst also looking after their all-important workforce. The ICO makes a clear point that Data Protection laws will not prevent businesses from making appropriate adjustments in order to help deal with the crisis; stating that organisations must on a case by case basis weigh up risks to their businesses, people and wider society against individuals' rights to privacy.

ICO looks to the future

The ICO has subsequently also issued a further statement setting out its priorities and its envisaged role as "both an enabler and a protector"; enabling innovation, but also looking to ensure people's privacy is protected.

In broad terms they say their focus will be on the following areas:

— Protecting citizens and businesses during the COVID-19 crisis, particularly frontline workers and any who are especially vulnerable at this time.

— Supporting economic growth and digitalisation by offering practical guidance to enable businesses to grow and offer services in compliance with the law.

— Proportionate surveillance; the ICO will be keeping a close watch on contact tracing, testing, and the implications of any surveillance measures brought in to combat the pandemic's spread.

— Enabling good practice in AI by advising on ways in which privacy considerations can be built into AI, and the way it is employed across the digital economy.

— Encouraging transparency to increase public confidence and engagement in the decisions taken about how personal data is used, and how those decisions affect people's rights.

Meanwhile, also showing the need to reprioritise in these exceptional times, they have stated that they have paused their investigation into real time bidding and the Adtech industry. Their concerns remain however, and they aim to restart when the time is right.

United Kingdom

Contact tracing apps

The UK is one of a small number of countries who have, so far, rejected decentralised contact tracing apps in favour of a centralised system. The government's position is that a centralised system will make the app more effective and enable them to better respond to, and combat, the spread of the virus.

The app has been undergoing initial field testing on the Isle of Wight, and the ICO is also assisting in its development by providing feedback on the app's Data Protection Impact Assessment.

Questions have been raised as to whether or not sufficient justification has been provided by the government for the allegedly high level of interference with fundamental rights posed by the app. There have also been calls by the parliamentary Joint Human Rights Committee for contact tracing to be put before parliament and placed on a statutory footing. The Committee have sent a draft bill to the Health Secretary.

Brexit

The UK remains in the post-January 2020 transitional period that is due to end on 31st December 2020. The GDPR is still in force during this period, and is likely to be adopted into UK law and to largely continue to apply after the transition period.

However, the situation does remain relatively uncertain and negotiations are ongoing, although clearly interrupted to some degree by the outbreak of COVID-19. The ICO will update its guidance as appropriate, and organisations are advised to monitor the regulator's website.

United Kingdom

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