KPMG

Data privacy newsletter

KPMG Global Legal Services

January 2021

Contents

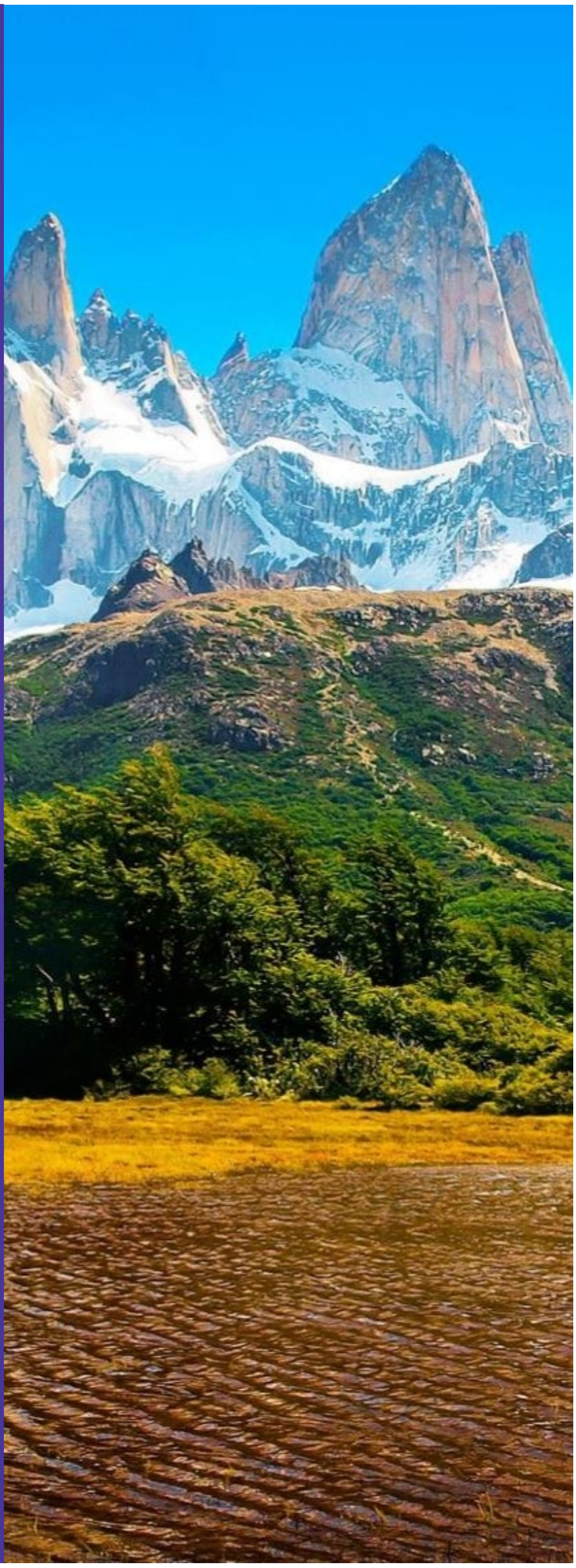
Introduction

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

KPMG's global network enables us to bring you various snapshots of recent developments in a selection of the jurisdictions. We live in fast changing times in this area. Our articles seek to demonstrate the state of development of the law in various jurisdictions whilst also showing the very broad impact that data protection law has. In this edition topics include regulatory actions and statistics, marketing, surveillance, data breaches, privacy impact assessments, new obligations for employers and social media issues.

Argentina

A. Serious infringement to Personal Data Protection



Serious infringement to Personal Data Protection

Court confirms fine imposed by the Data Protection Authority

On October 15, 2020, the Federal Court in Administrative Litigation No. 8 confirmed the penalty imposed on an Argentine corporation consisting of ARS 50,001, and the closure of the databases used to prepare its credit report.

The relevance of this decision is based on the fact that it is the first time that the courts confirm an administrative decision issued by the Data Protection Authority.

In Argentina, personal data is protected by the Data Privacy law. The main purpose of this law is the general protection of the personal data contained in files, registers, data banks, or other technical means of data processing, either public or private, destined to reports, to guarantee the right to honor and privacy of the people, as well as the access to the information that is registered on them, in accordance with the provisions Argentine Constitution. The provisions of this law are also applicable, as pertinent, to legal entities.

In the case under analysis, the Data Protection Authority concluded that the company's credit report violated the principle of data quality set forth in the Argentine Data Privacy Law. Furthermore, it was considered that the report included data on "possible relatives" and "possible neighbors" that, on the one hand, were neither adequate nor relevant to evaluate the credit situation of the owner of the data, and on the other, were excessive in relation to the area and the purpose for which they were collected. In this regard, the Data Protection Authority concluded that the transfer of personal data was illegitimate, since such specific data was not related to the business.

Due to the violation of several sections of the Argentine Data Protection Law, the Data Protection Authority understood that the company had committed a serious offense and that penalties should be applied.

Although the company filed a claim for invalidity, the judge considered that the administrative act issued by the Data Protection Authority was valid, since it met the relevant requirements of the Administrative Procedure Law. For this reason, the claim was rejected and the penalty imposed was ratified. The company filed an appeal and the case is now pending before the Court of Appeals.

Argentina

If you have any questions, please let us know

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

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

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

Belgium

A. Use of camera surveillance: unlawful filming of public domain and private property

Belgium

Use of camera surveillance: unlawful filming of public domain and private property

The Belgian Data Protection Authority ('BDPA') recently issued a decision regarding camera surveillance by a natural person. It concerned the unlawful filming of the public domain and private property with security cameras. The Belgian DPA decided that the defendants violated the provisions of the GDPR, resulting in a fine of 1.500 EUR.

The Belgian DPA received a complaint from two data subjects regarding the unlawful filming of the public domain and their private property with security cameras. In this case, the defendants had a video surveillance system installed on their premises consisting of five cameras. The neighbors of the defendants filed a complaint with the BDPA as certain cameras filmed part of the public domain and the private property of the plaintiffs - which the plaintiffs were informed of by a third party (independent expert) in the course of an ongoing environmental lawsuit between the plaintiffs and the defendants.

Those images provided in the court case by the independent expert were - according to the plaintiffs - not only the evidence of unlawful recording of the public domain and their private property, but also of the unlawful transmission of the recordings of those images to unauthorized third parties (i.e. the independent expert).

In its decision, the BDPA emphasized that the European Court of Justice has previously confirmed that the recording of images of persons with surveillance cameras falls under the concept of 'personal data' within the meaning of the EU data protection standards. The surveillance by means of video recordings of individuals, which are stored, is an automated processing of personal data within the meaning of Article 2(1) of the GDPR. The processing of personal data in this context must therefore also benefit from the same level of protection as provided for by the GDPR.

Regarding the filming, the defendants invoked their legitimate interest ("maximize the protection of their property") as legal basis. The BDPA decided that the conditions for the use of this legal bases for processing were not fulfilled.

Belgium

Firstly, the processing of the personal data was not necessary for the purposes of the legitimate interests as less intrusive measures were possible, e.g. by the adjustment of the position of the surveillance cameras.

Secondly, the BDPA stated in its decision that such interests cannot override the fundamental rights and freedoms of the data subject. The fact that the surveillance cameras had been set up in a manner of continuous monitoring, i.e. 24 hours a day, 7 days a week, of the public domain and the plaintiffs private property, constituted a serious infringement according to the BDPA.

In addition, the BDPA indicated that, the filming did not only interfere with the (fundamental) rights of the plaintiffs. Other people, such as the children of the plaintiffs and drivers passing by on the road in front of the defendants' house, were also being recorded and therefore their (fundamental) rights were also violated.

Regarding the transmission of the recordings, which is a processing activity in the meaning the GDPR, the BDPA decided that no legal ground existed for the transfer of the recordings to the independent expert and thus violated the provisions of the GDPR.

For both infringements, the Belgian DPA issued a reprimand and imposed a fine of EUR 1,500.

Belgium

If you have any questions, please let us know

Frank Cleeren
Partner
K Law Belgium
T: +32 (0)11 28 79 77
E: fcleeren@klaw.be

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

Bart Putteman
Junior Associate
K Law Belgium
T: +32 (0)2 7084157
E: bputteman@klaw.be

China

A. China has made significant progress for legislation of personal data protection

B. China's draft Personal Information Protection Law has extra territory jurisdiction

C. China intends to facilitate cross-border transfer of personal data

D. The cost of non-compliance would be extremely high

China

China has made significant progress for legislation of personal data protection

The legislation of China data protection laws has been evolving in past years. There are significant progresses recently. The release of draft Personal Information Protection Law ("draft PIPL ") is a new milestone.

On 21 October 2020, the Standing Committee of China's National People's Congress (SCCNPC) released the draft PIPL for public comments. The draft PIPL is China's first unified legislation for protecting personal data and will become one of the three essential laws of China's data protection law system when implementing in the near future. It develops and aligns with general principles of the Civil Code (effective as of 1 January 2021), Cybersecurity Law (effective as of 1 June 2017) and Data Security Law (still pending for public comments). In addition, the national technical standard Information Security Technology Guidelines of Personal Information Security Assessment was officially published on 19 November 2020, which would much help cross-border transfer of personal data.

The draft PIPL mainly addresses personal data processing, cross-border transfer of personal data, the rights of data subjects for data processing, data processor obligations, the supervisory authority in charge of personal data protection, and legal liability of non-compliance.

Furthermore, the draft PIPL reiterated principles of personal data processing, which are basically consistent with those of international practice like GDPR. These principles generally include lawfulness and fairness, transparency, purpose limitation, minimum necessary, accuracy and integrity, security and accountability. But the draft PIPL only provides the obligations of data processor. It appears that it does not intend to distinguish the obligations of data controller and data processor as GDPR.

On 21 December 2020, the SCCNPC has published its 2021 legislative. The plan aims to continue to review the draft PIPL and draft Data Security Law. We suppose the PIPL and Data Security Law may be officially promulgated by SCCNPC this year.

China's draft PIPL has extra territory jurisdiction

The draft PIPL has extra territory jurisdiction over overseas data processing activities.

With reference to General Data Protection Regulation ("GDPR"), the draft PIPL also can be applied in three situations on processors located outside China, which include actions for the purpose of providing goods or services, analyzing or assessing individuals located within China, as well as certain other situations required by relevant laws and regulations.

In addition, if overseas organizations want to process the personal data in China, they must set up a specialized agency or designate a representative in China to take the responsibilities of performing relevant matters. In this way, the name of agency, name and contact information of the representative are required to report to data protection authority.

It is worth noting that, the extent of the influence of the GDPR remains strong in the draft PIPL of China. Obviously, China intends to increase protection level of personal data to align with international standards.

China

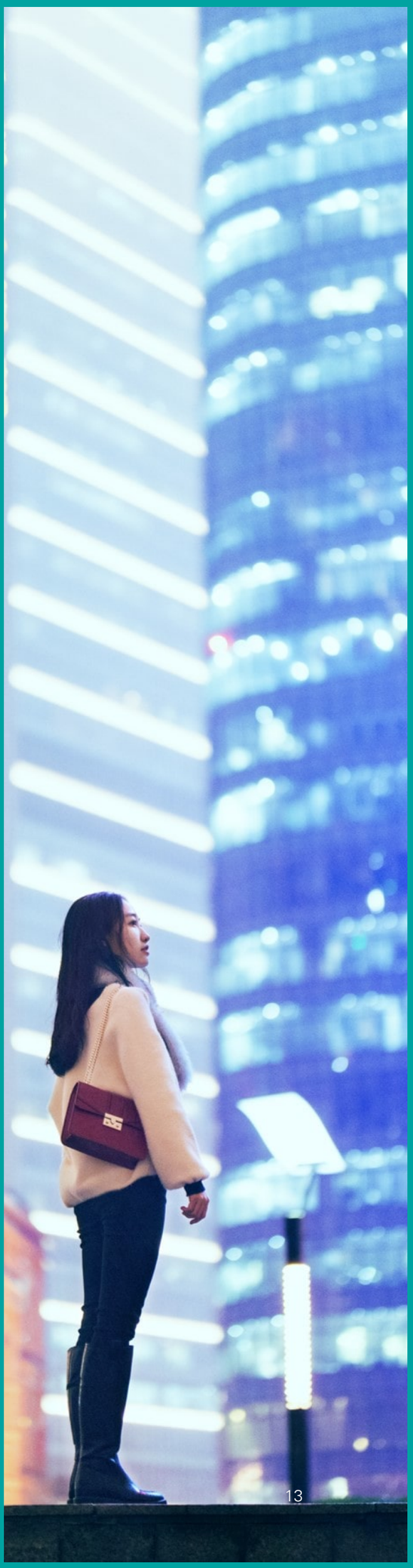
China intends to facilitate cross-border transfer of personal data

The draft PIPL provides more options for international organizations to cross-border transfer of personal data.

Under the previously published draft 2017 Guideline Concerning the Security Assessment of Cross-border Transfer of Personal Information and Important Data as well as draft 2019 Measures on Security Assessment for Cross-border Transfer of Personal Information, the cross-border transfer of personal data must pass security assessment.

Cross-border transfer of personal data is one of the key concerns for most international organizations, comparing with the above previous draft regulations, the PIPL relaxes the previous single stringent route of cross-border transfer, i.e. passing the security assessment conducted by the Cyberspace Administration of China. The PIPL provides three additional routs of cross-border transfer of data (1) certification by third party professional certification institutions; (2) signing contracts with overseas recipients; and (3) meeting other conditions stipulated by laws, administrative regulations or the Cyberspace Administration of China.

Under the PIPL, it is obvious that it's more convenient for international organizations to process personal data in China. However, many practical issues still need to be further clarified. For example, what are the qualifications and specific operation guidelines of third-party certification organizations which are eligible for such certification? Are there any standard contract clauses like GDPR while entering into contracts with overseas recipients? What are other conditions stipulated by laws, administrative regulations or the Cyberspace Administration of China? Therefore, international organizations need to consider their best practices to process the cross-border transfer of data legally in consideration of all the possible factors.



The cost of non-compliance would be extremely high

The supervisory authorities have been intensifying enforcement of protecting personal data recently. The enforcement primarily focuses on illegal collection, processing, storage, and use of the personal data. The cost of non-compliance would be extremely high.

Since 2019, the China supervisory authorities started to carry out a series of special actions on APPs' illegal collection and use of personal data. A number of APPs were ordered to stop operation due to the non-compliance problems.

The draft PIPL does not specifically provide possible legal liabilities for each acts of violation. But it provides, under severe circumstances, the possible liabilities include cancelling business licenses, suspending business operations, huge amount of fines for organizations and possible fines for individuals. The capped amount of fines for serious violations has been significantly increased compared with other laws like Cyber Security Law, which can be as high as RMB 50 million or 5% of the previous year's turnover, while the "turnover" and "serious circumstances" are not yet clearly defined. Moreover, the person directly in charge and other directly liable individuals may also be fined from RMB 100,000 to 1 million. But the PIPL does not specify the circumstances under which individuals need to bear their personal responsibilities for the organization's violations.

Under the draft PIPL, violations may be recorded into the Social Credit Rating System (SCRS) and be disclosed to the public. This will definitely have serious negative impacts on their reputation of public image, thereby causing disasters to their business operation. But the draft PIPL does not further clarify whether all violations or only serious violations will be recorded into the SCRS.

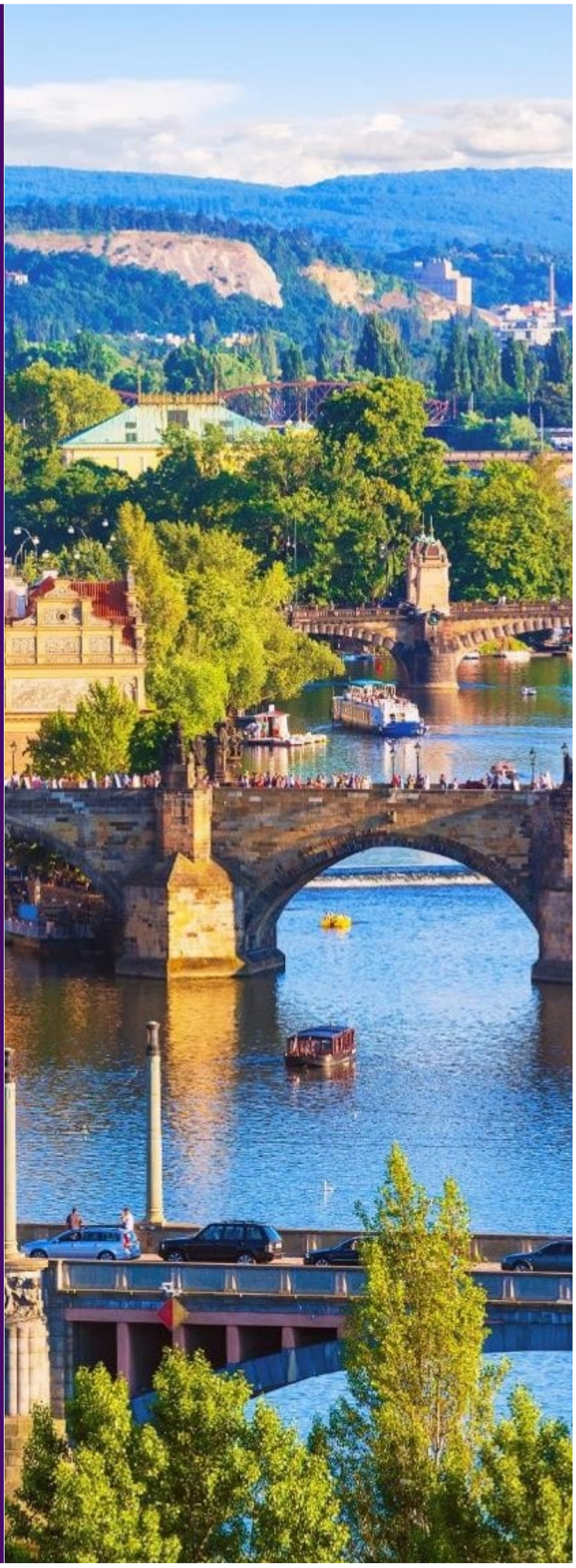
China

If you have any questions, please let us know

Rocky Wu
Partner
Shanghai SF Lawyers China
T: +86 (21) 52031587
E: rocky.wu@kpmglegal.com.cn

Czech Republic

A. New DPIA Methodology Released



Czech Republic

New DPIA Methodology Released

The Czech Data Protection Authority introduced new methodology (guidelines) for carrying out data protection impact assessments (DPIA). This tool should serve both private and public personal data controllers for DPIA purposes.

This initiative follows up on the Data Protection Authority´s revelations that controllers often do not adequately and correctly use the tools for personal data protection introduced by GDPR. This is particularly the case when it comes to more complex projects and agendas concerning personal data (such as DPIA).

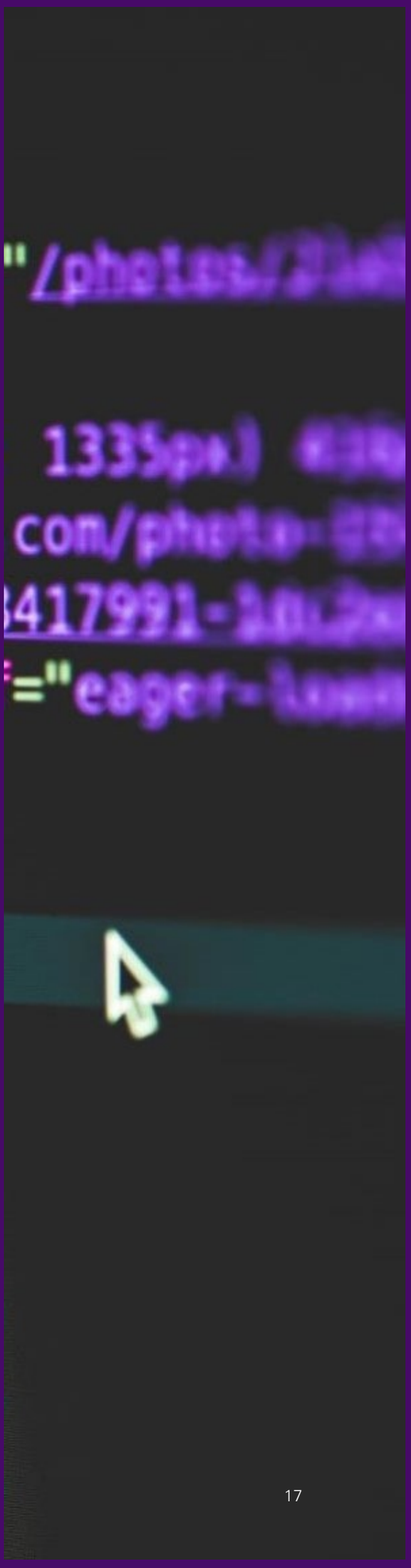
It is not rare that the controllers carried out the DPIA only in the form of a verbal assessment. Such assessment was usually without any specific information concerning the description of the threats, impacts on privacy and proposed technical and organizational measures.

The new DPIA methodology includes practical examples and guidance as to what kind of analysis should be conducted, when and who carries out the analysis, what threats and risks may arise etc. It divides the controller´s approach while carrying out DPIA into four phases.

The first phase includes gathering the information on processing. The following step entails an analysis of whether the DPIA is necessary. If yes, in the third phase, the DPIA is carried out. Finally, the monitoring of compliance with the measures taken and a regular review of the DPIA should be made.

The methodology also includes a detailed description of the DPIA process from the controller´s perspective. The process itself is divided into 8 parts and the goal is to lead the controller through the DPIA process step by step while using practical examples. This covers a thorough description of the envisaged data processing operations, through to risk assessment and external consultations and necessary approvals.

Lastly, this methodology is not legally binding and has a form of recommendation. This means that it is permissible for a subject to carry out the DPIA to choose a different methodology and cover the necessary requirements in line with the GDPR. The methodology is primarily intended for data controllers, but of course also data processors may use it.



Czech Republic

If you have any questions, please let us know

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

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

Martin Čapek
Lawyer
KPMG in the Czech Republic
T: +420 222 123 967
E: mcapek@kpmg.cz

Germany

A. New rights and obligations for German works councils regarding data protection and IT

B. Holding video conferences based on the latest guidelines laid down by the German Conference of Data Protection Authorities.

Germany

New rights and obligations for German works councils regarding data protection and IT

On 21 December 2020 the Federal Ministry of Labor and Social Affairs (BMAS) has published the draft legislation for an amendment of the German Works Constitution Act (Betriebsverfassungsgesetz).

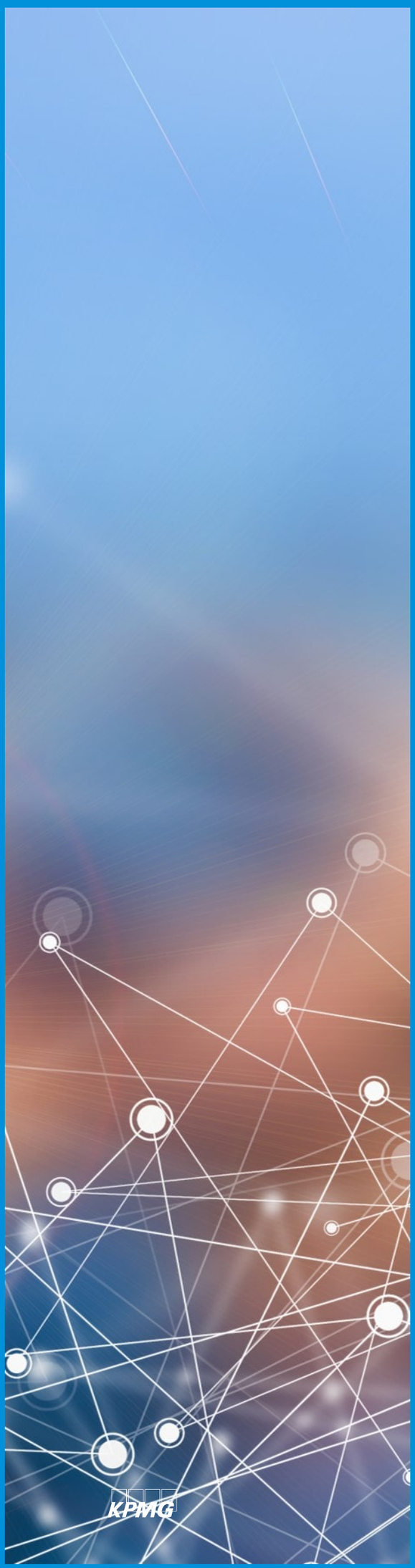
The German Federal Ministry of Labor and Social Affairs has published the draft legislation for an amendment of the German Works Constitution Act. The draft contains inter alia the following provisions regarding data protection and IT:

- The works council is required to comply with data protection regulations when processing personal data. Insofar as the works council processes personal data in order to fulfill tasks within its competence, the employer is regarded as the data controller (in the meaning of Art. 4 No. 7 GDPR). Employer and works council are obligated to mutual support complying with data protection law. (Sec. 79 a Works Constitution Act)

- If the employer intends to use or introduce technical equipment suitable for monitoring the behavior or performance of employees, the works council may consult an expert in information and communication technology (Sec. 80 para. 3 Works Constitution Act).

- Before a planned use of artificial intelligence, the employer must inform the works council and discuss the measure with him (Sec. 90 para. 1 No. 3 Works Constitution Act).

- Guidelines for personnel selection with the use of artificial intelligence require the approval of the works council (Sec. 95 para. 2.a. Works Constitution Act).



Comment

The regulation raises practical issues:

The processing of personal, sometimes sensitive, employee data is one of the core tasks of works councils. They therefore have a special responsibility to ensure compliance with data protection regulations. When processing personal data, works councils act as an institutionally dependent part of the employer responsible for compliance with data protection. The regulation clarifies the unclear legal data protection role of German Works Councils. However, the questions that now need to be clarified for the German works council's obligations under the GDPR are: What happens if the works council denies its support? Does the works council still need to observe time limits according to GDPR, e. g. when responding to data subject requests? What happens if data protection obligations are violated due to insufficient support of the works council and a fine is imposed on the employer as a result? The new regulation states that the employer is the data controller only "as far as" the works council performs his tasks within his competence. What happens, if the works council processes personal data beyond his competence; does the employer´s controllership end?

The increasing complexity of work processes associated with digitization also affects the tasks of works councils. They must be able to understand, evaluate and help shape complex information technology contexts. The Works Constitution Act gives them the opportunity to draw on the expertise of employees in the company. Insofar as this is not sufficient and it is necessary for the proper fulfillment of their tasks, works councils can consult experts after agreement with the employer.

Decisive for the acceptance of AI in the company is, above all, the early involvement of employee representatives. When planning work processes with AI, the employer must inform the works council of this and consult with him. One area in which AI is already increasingly being used today is personnel selection. Here, so-called algorithmic decision-making systems (ADM systems) are used. The works council must be involved in this process.

Germany

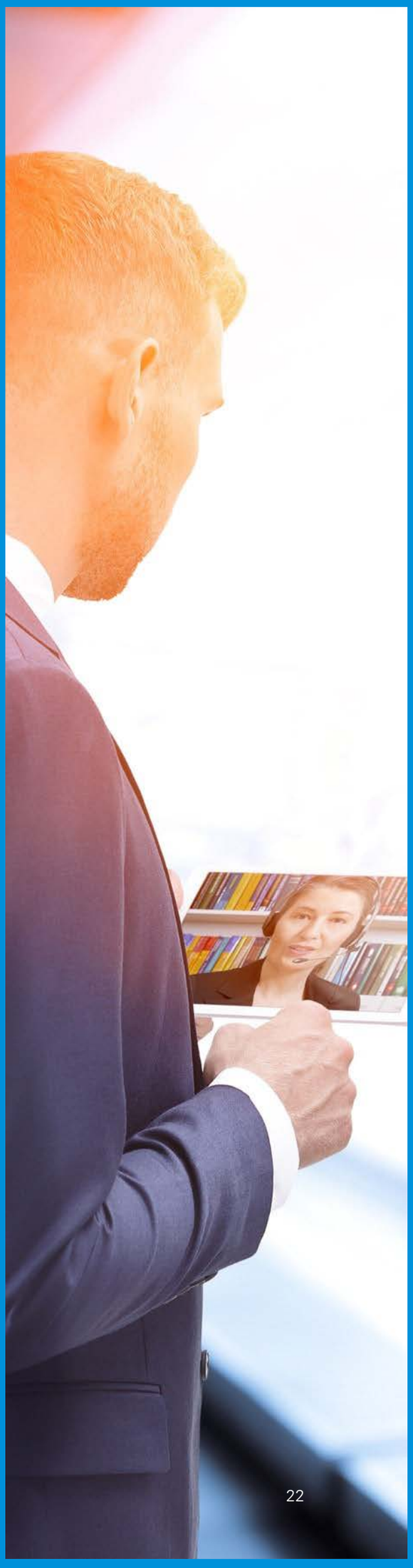
Holding video conferences based on the latest guidelines laid down by the German Conference of Data Protection Authorities.

On October 23th, the German Conference of Data Protection Authorities has issued guidelines on data protection requirements for holding of videoconferences by companies, public authorities and other organizations.

During video conferences personal data of the participants is being processed by the controller. The range of personal data to be processed is wide: The personal data being processed include, for example, images, sounds, statements, the environment (home, workplace or other location). Furthermore, metadata of the conduct of the communication, data of professional contacts, of working hours and of work performance can also be processed on the basis of the data collected during one or more video conferences. In addition, there is personal data in text messages of the participating persons and documents discussed and made visible in this context. These data can refer to the participating persons themselves, but also to non-participating persons inside and outside the organizations (data subjects).

The before mentioned Guidelines laid down by the German Conference of Data Protection Authorities provide that the Controller (person responsible for conducting the videoconference) shall ensure the following principles while processing personal data of the data subjects:

First of all, the controller is obliged to assess if and to what extent he is permitted to process personal data after all. The controller requires a legal basis for the processing of personal data of the data subjects according to Article 6 GDPR. Depending on the context of the processing situation, the legal basis may result from Article 6 para 1 sentence 1 let. a), b), e), f) GDPR, possibly also in conjunction with national law. The controller shall examine the respective legal basis in detail.



Principle of data minimization: The controller shall assess to what extent the data processing associated with the specific use of the conferencing system can be limited to achieve its purposes. The controller is able to ensure this by thoroughly selecting the systems used and by taking (other) technical and organizational measures.

Before operating or using a video conferencing service, the roles and responsibilities of the parties involved shall be clearly allocated and explicitly defined in order to ensure compliance with the provisions of the GDPR.

If the controller uses tools from a provider, the controller shall assess its own data protection relationship with this provider and, if necessary, conclude a corresponding data processing in accordance with Article 28 GDPR.

The controller shall inform the data subjects according to Article 13, 14 GDPR and be able to ensure the data subjects' rights in accordance with Article 15 et seq. GDPR.

In conclusion the possibility of using videoconferences from various providers (some of them are very user friendly but not very strict on GDPR obligations) is a necessary tool for modern designed workplaces but this does not exempt the controller from its obligations under data protection law. However, the latest guidelines laid down by the German Conference of Data Protection Authorities do not provide any more support than stating the already well known obligations a controller has under the GDPR.

Overall, it is the sole responsibility of the controller to check the compliance of each tool with the above mentioned criteria and to document the assessment.

Germany

If you have any questions, please let us know

Maik Ringel
Senior Manager
KPMG law
T: +49 (0) 341 22572 546
E: mringel@kpmg-law.de

Ariane Loof
Senior Manager
KPMG law
T: +49 (0) 30530199 625
E: aloof@kpmg-law.de

Greece

A. Cameras in public and private areas

B. Photos from social media protected as personal data

C. Protection of Personal Data and COVID-19 (i. work from home, ii. Distance learning)

D. Fines imposed by the Hellenic Data Protection Authority in 2020

Cameras in public and private places

Cameras in public areas

In September 2020, a Precedential Decree (PD 75/2020) was pupbished, providing the circumstances under which cameras are lawfully placed in public areas.

This PD establishes the rules for the installation and operation, in public places, of sound or video recording or recording surveillance systems, to the extent that personal data is processed. Such installations are legitimate for the purpose of suppressing criminal offenses (as well as proving the commission of criminal offenses and identifying the perpetrator) and traffic management (i.e. dealing with road network emergencies, regulating vehicle traffic and preventing and managing road accidents). Such an installation may be carried out only if the above purposes cannot be carried out by other, milder means and should be limited to the specific area for which the data controller deems it necessary. All data collected should be kept for a maximum period of fifteen (15) days from collection, unless retention is required for a longer period.

Cameras in private areas

The collection and processing of personal data through CCTV, installed in private spaces by an individual solely for the exercise of personal or domestic activities is legal.

This is not the case, when CCTV is installed in a private area, enabling however the recording of public areas (such as the surrounding municipal or community roads, or other neighboring third-party private spaces). The possibility of collecting, storing or further processing the image of third parties who use these public spaces, definitely constitutes a violation of the GDPR on behalf of the owner of these CCTVs, since it is no longer a processing of personal or domestic activities of the individual acting in his private space, but rather processing of personal data of third parties. This processing falls within the scope of Greek law for the processing of personal data and since it offends the personality and privacy of the third party, and it is therefore prohibited.

However, the above processing is exceptionally allowed, without the consent of the data subject , provided that the following conditions are cumulatively met: a) it is intended to protect persons or goods, b) it is absolutely necessary to achieve the purpose for which it is collected, in the sense that said purpose cannot be achieved as effectively as other measures less burdensome for the processor; c) the legitimate interest of the controller clearly outweighs the rights and interests of the controller and the processing does not prejudice their personal freedoms; and d) by posting clear signs, he has pointed out to subject to processing the space that falls within the scope of the camera and video recorder, as required by law.

Greece

Photos from social media as personal data

Photos from sociał media constitute personal data that require the consent of the subject in order to be lawfully processed. Alternatively, without said consent, they could be processed only by invocation and proof of a superior legal interest which must be protected. As long as there is a privacy setting that allows photos to be viewed only by online "friends" and not publicly by third parties, the published photos are considered protected personal data and should be protected accordingly. Consequently, the invocation and promotion of such data by a third party without the consent of the subject of personal data and without meeting one of the conditions set by law is a prohibited processing.

Greece

COVID-19 and personal data

Protection of personal data during work from home

Due to the restrictive measures imposed to prevent the spread of COVID-19, many organizations and companies encouraged and / or obliged their staff to work from home, utilizing relevant capabilities of technology.

Teleworking, is defined as working remotely (i.e. without physical presence in workplace) using the necessary information and communication technologies.

The Hellenic Data Protection Authority, with the aim of raising the awareness of controllers, processors, employees and the general public regarding the risks related to the protection of personal data, and highlighting at the same time the obligations arising from the General Data Protection Regulation and the respective Greek law set out specific Guidelines. According to these Guidelines, each organization / company must define and support specific procedures for teleworking that must take into account the nature and severity of the risks to the protection of personal data arising from remote work. The organization must also adequately inform, train and assist its employees in the implementation of these procedures, given that many users are unfamiliar with the technologies supporting teleworking and the associated risks. For this purpose, the contribution of the Data Protection Officer (DPO) is valuable. Finally, it is pointed out that the obligations of the institutions regarding the protection of their employees' personal data acquire special weight in the case of teleworking, since they are located in their own homes and therefore have a higher expectation for the protection of their privacy.

Protection of personal data during distance/on-line learning.

For the protection of personal data both of educational staff/teachers and students, the main key features of the specially configured platform of the Greek Ministry of Education are twofold: i the recording / storage feature has been disabled, and ii "locked" digital rooms have been created, in which the teacher has the exclusive entrance control.

The metadata that may be generated (course time and duration, number of participants) from the above processing are used exclusively for research or statistical purposes.

Greece

Fines imposed by the Hellenic Data Protection Authority in 2020

In 2020, the Hellenic Data Protection Authority imposed the following fines:

- Fine of EUR 8 000.00 imposed to a private individual for violation of article 5 if the GDPR (in particular for failure to comply with data processing principles) since as a data controller he monitored public space using CCTV cameras, which was outside the scope of the surveillance system.

- Fine of EUR 3 000.00 imposed to a candidate for parliamentary elections for violation of article 15 of the GDPR (in particular non-compliance with lawful basis for data processing) since the data subject, when attempted to use its right to access since it received telephone calls related to a candidacy for parliamentary elections, didn't receive any information regarding that right.

- Fine of EUR 5 000.00 imposed to an educational entity/college for violation of article 5 if the GDPR (in particular for failure to comply with data processing principles) since it had directly contacted the complainant by telephone and processed its personal data in a non-transparent way.

- Fine of EUR 8 000.00 imposed to a special education center for violation of articles 15 and 58 of the GDPR (in particular non-compliance with data access obligation) since the data controller unlawfully restricted data access to the complainant about a child's data and tax information.

- Fine of EUR 5 000.00 imposed to a Power Supply Corporation for violation of article 15 of the GDPR (in particular non-compliance with data access obligation) since the company failed to fulfil the data subjects' rights referring to the processing of their personal data (requesting a copy of the personal data processed)

- Fine of EUR 15 000.00 imposed to a Private Maritime company for violation of article 5 (1) (a), (2) of the GDPR (in particular non-compliance with lawful basis for data processing) since the company unlawfully introduced a video surveillance system at the workplace to monitor employee activity. The Hellenic Data Protection Authority argued that the installation of the system was unlawful because the employees were not notified of the existence of the system.

If you have any questions, please let us know

Liana Kosmatou
Director
Papacostopoulos – Grigoriadou and Associates Law Firm
T: +30 2106062297
E: lkosmatou@cpalaw.gr

Penny Vithoulka
Senior Manager
Papacostopoulos – Grigoriadou and Associates Law Firm
T: +30 2106062205
E: pvithoulka@cpalaw.gr

Poland

A. An incidental security review cannot be qualified as regular testing of technical measures

B. Publication of private addresses of politicians and judges on Twitter

C. A reprimand for revealing a list of people being under quarantine

Poland

An incidental security review cannot be qualified as regular testing of technical measures

The Polish data protection authority (DPA) imposed a fine on a telecommunications services provider in the amount of PLN 1.9 million for failure to implement appropriate technical and organizational measures ensuring the security of the processed data.

DPA found that the provider violated the principles of data confidentiality and accountability set out in the GDPR. The provider did not carry out regular and comprehensive tests, measurements and evaluation of the effectiveness of the technical and organizational measures used to ensure the security of the processed data. Actions in this area were undertaken only in connection with the emerging suspicions of a vulnerability or in connection with organizational changes.

As a result of the above violations of personal data protection, an unauthorized person obtained access to customer data from one of the databases.

During the proceedings conducted by DPA, it turned out that the exchange of data between applications in the IT system had to take place after the verification of certain parameters from the registration applications of prepaid service customers. In practice, this verification did not work properly and the mechanism had not been tested prior to its implementation.

DPA decided that the implementation of the data processing system for use without properly functioning validation of the assumed parameters is a gross violation of the controller.

For the purposes of calculation of the penalty, DPA took into account that the provider's breach is of a serious nature, as it causes a high risk of negative effects of legal protection for a large number of people (e.g. risk of identity theft). It should be remembered that despite the fact that unauthorized persons had short-term access to the systems, it was still sufficient to download a large amount of data. In addition, the breach itself was long-term - the vulnerability of data leakage had existed for a long time.

Poland

Publication of private addresses of politicians and judges in social media

In connection with the publication in social media of the private addresses of pro-life activists, politicians and judges, the DPA took immediate steps to protect the personal data and privacy of these people.

According to DPA, the posting of private address and contact details of pro-life activists, politicians and judges by users of the social media network is an action leading to the disclosure of a wide sphere of privacy, and thus causing threats to health and life, such as possible acts of violence and aggression targeted at these people and their family members.

In connection with the above, DPA immediately asked the Irish supervisory authority competent for the processing of personal data via social media carry out the investigation. Pointing out to the huge scale of threats, attention was drawn to the necessity to verify the response time to reported irregularities and the possibility of introducing automated solutions to counteract the rapid promotion of such content by other portal users.

DPA also applied to prosecution authorities with a notification that users of the Twitter website, who made available twits containing private data of the above-mentioned persons, had committed the crime on the processing of personal data without any legal basis.

DPA asked as well the Polish authorities to report the case to prosecution authorities under special supervision due to the escalation of conflict and aggression, which cause a high risk of violating the life interests of both persons whose data is published on social media and their family members.

Poland

A reprimand for revealing a list of people being under quarantine

The Polish data protection authority, after carrying out ex officio proceedings related to the breach of personal data protection of persons subject to medical quarantine by providing unauthorized recipients with a list containing the addresses of residence of persons subject to medical quarantine, reprimanded the company dealing with waste management and ordered to notify those persons.

DPA received a letter informing on the public disclosure of the list containing the addresses of residence of persons who are quarantined by a decision of competent authorities and compulsory quarantine due to crossing the country border, as well as address details of people undergoing home isolation in connection with the confirmed COVID-19 infection.

The company stated, in particular, that it conducted a risk analysis taking into account the circumstances related to the non-compliance by processors with the above-mentioned lists of procedures in force in the company and circumstances related to the theft or removal of data. Moreover, the controller expressed the view that the lists received included only administrative (police) addresses, and did not include names, surnames and other data allowing the identification of a natural person.

DPA considered that the information regarding: the name of the city, street name, building / flat number as well as placing a person under medical quarantine, constitute personal data within the meaning of the provisions of the GDPR, and the fact that people are under quarantine constitutes personal data of a special category regarding health. DPA found also that the confidentiality of the processed data was breached in the course of the performance of the employee's duties of the person responsible for supervising the printed list left on the desk without proper supervision. During this time, another employee recorded the list in the form of a photo and shared it with another person.

In DPA's opinion, the provisions included in the controller's risk analysis, which largely refer only to the signing of relevant statements and documents by employees, are insufficient and inadequate to the risks related to the processing of special category data.

DPA also noted that a one-off and cursory analysis also means that the controller does not take actions aimed at, inter alia, ensuring regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

Poland

If you have any questions, please let us know

Magdalena Bęza
Of Counsel
D. Dobkowski spółka komandytowa
T: + 48 22 5281405
E: MBeza@kpmg.pl

Piotr Dziekoński
Junior Associate
D. Dobkowski spółka komandytowa
T: +48 22 5283289
E: pdziekonski@kpmg.pl

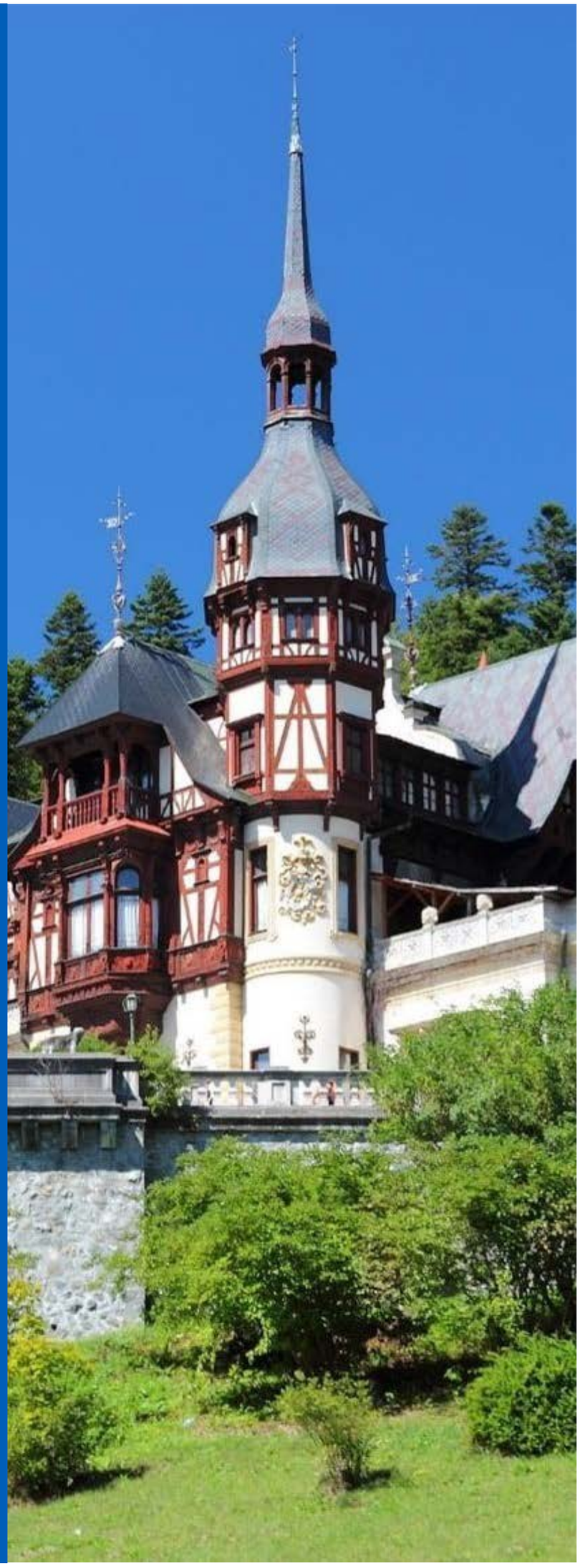
Romania

A. Position of the Romanian Data Protection Authority on retaining copies of clients' identity documents

B. Statistics regarding the control activity of the Romanian Data Protection Authority

C. Data processing by homeowners' associations

D. Latest sanctions imposed by the Romanian Data Protection Authority



Romania

Position of the Romanian Data Protection Authority on retaining copies of clients' identity documents

The Court of Justice of the European Union confirmed the position of the Romanian Data Protection Authority regarding the illegality of controller's storage of identity documents of its clients, without their express consent on the occasion of concluding contracts for providing telecommunications services. The request for a preliminary ruling was submitted to the Court of Justice of the European Union by a Romanian court, following a dispute between a Romanian mobile phone network operator and the Romanian Data Protection Authority.

The Court of Justice of the European Union stated that *"a contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent to that collection and storage:*

• where the box referring to that clause has been ticked by the data controller before the contract was signed, or

• where the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or

• where the freedom to choose to object to that collection and storage is unduly affected by that controller, in that it requires that the data subject, in order to express his or her refusal to consent to such processing, must complete an additional form setting out that refusal."

Statistics regarding the activity of the Romanian Data Protection Authority

During the period January 2020 – September 2020 the Romanian Data Protection Authority received a number of 3,952 complaints, 176 notices and 128 data breach notifications, based on which investigations were opened.

Following the investigations carried during this period, 23 fines were imposed, amounting of a total of 70,900 EUR.

Also, 46 reprimands were issued and 42 corrective measures were imposed.

Corrective measures were also applied during the investigations, such as:

- to comply with the data subject's requests to exercise his or her rights pursuant to the GDPR;
- to bring processing operations into compliance with the provisions of the GDPR;
- reviewing and updating the implemented technical and organizational measures, including the working procedures regarding the protection of personal data, as well as the implementation of measures regarding the regular training of persons acting under the authority of the controller, regarding controller's obligations according to GDPR, including regarding the risks involved in the processing of personal data, depending on the specificity of the activity;
- conducting a risk assessment for the rights and freedoms of persons including the classification in a degree of risk, taking into account the nature, scope, context and purposes of the processing.

Data processing by homeowners' associations

The Romanian Data Protection Authority issued recommendations regarding the personal data processing activities carried out by homeowners' associations.

The Romanian Data Protection Authority emphasizes that homeowners' associations act as controllers and have the obligation to comply with the provisions of the GDPR.

The Romanian Data Protection Authority mentions that the purpose and means of data processing by homeowners' associations may be expressly established by the laws governing their establishment, organization and operation or may be established by the association, being justified by its legitimate interest. Also, in some cases, data processing may be based on the consent of the data subjects.

The Romanian Data Protection Authority establishes that homeowners' association must analyze the data processing activities carried out and establish the legal basis of the processing and take all necessary measures to respect the rights of data subjects and ensure security and confidentiality of the personal data.

With regard to the appointment of a data protection officer, the Romanian Data Protection Authority considers that they do not have an obligation to appoint a DPO.

The Romanian Data Protection Authority has identified that the purposes for which these entities collect and process personal data are mainly related to the following activities:

• Installation of a video surveillance system

According to the Romanian Data Protection Authority, this measure can be taken based on the legitimate interest of the association, e.g. for ensuring the security and protection of persons, goods and values, of buildings and public utility installations.

Regarding the obligation to inform the data subject, the Romanian Data Protection Authority mentions that an appropriate icon should be installed, containing a representative image, positioned at a reasonable distance from the places where the surveillance equipment is located, so that to be seen by anyone.

Regarding the storage period, the Romanian Data Protection Authority recommends that it not exceed 30 days. Exceptions may be duly justified situations in which events have occurred that require the storage of only the relevant images for a longer period of time necessary to achieve those purposes (e.g. until the final settlement of a criminal case by the judiciary).

Regarding the installation of video cameras on each floor of the building, the Romanian Data Protection Authority considers that for the processing of the respective images it is necessary to obtain the consent of each tenant from that floor.

• Disclosure of data such as the name and surname of the tenants on the block notice board

According to the Romanian Data Protection Authority, in the absence of an express legal provision, the data may be disclosed only on the basis of the consent of the data subject.

• Registration of personal data in the real estate book

The Romanian Data Protection Authority mentions that, to the extent that there is a legal obligation in this regard, the data may be processed without the consent of the data subject.

Latest sanctions imposed by the Romanian Data Protection Authority [1/2]

In the last five months (August-December) the Romanian Data Protection Authority has completed several investigations and applied eleven fines amounting between 500 EUR and 100,000 EUR and two reprimands, as follow:

— Fine of 500 EUR applied to a homeowners' association for the illegal processing of the image of a data subject, from the video surveillance system, by posting on the block notice board. The Romanian Data Protection Authority also applied two reprimands for not adopting technical and organizational measures adequate for the protection of personal data collected through the video surveillance system and for the lack of a complete information notice regarding the personal data processed through the video surveillance system.

— Fine of 2,000 EUR applied to a controller for the violation of the personal data security measures. The fine was applied following the submission by the controller of a notification of a personal data breach consisted in the fact that, during the organization of an online event, the login data of some data subjects were erroneously transmitted to other e-mail addresses than those with which they had created an account on the electronic platform of the controller. This situation led to the disclosure and unauthorized access to the data of other participants in the event (e-mail addresses, usernames), with effects for a number of 1,300 users of the controller's platform.

— Fine of 3,000 EUR applied to a controller for not fulfilling the ordered corrective measure to send a response to the requests of the Romanian Data Protection Authority. The investigation was launched as a result of the fact that several petitioners notified the Romanian Data Protection Authority about the fact that they received by SMS commercial messages promoting the services of the controller's website without having consented to receive such messages.

— Fine of 2,000 EUR applied to an owners' association for not fulfilling the ordered corrective measure to send a response to the requests of the Romanian Data Protection Authority. The sanction was imposed following a complaint of the petitioner claiming that the request sent to the owners' association had not been answered.

— Fine of 3,000 EUR applied to a controller for the failure to adopt sufficient security measures to prevent the unauthorized access and disclosure of personal data of customers who placed orders on controller's website. At the same time, the controller was recommended to establish a shorter storage period of personal data related to customer accounts.

— Fine of 2,000 EUR applied to a controller for not fulfilling the ordered corrective measure to send a response to the request of the Romanian Data Protection Authority.

— Fine of 4,000 EUR applied to one of the Romanian mobile phone network operator for not responding within deadline to data subject's requests for exercising the access and erasure rights. At the same time, the Romanian Data Protection Authority applied a corrective measure to communicate a response to the petitioner to his requests regarding the measures adopted on their basis.

— Fine of 5,000 EUR applied to a controller for the failure to implement adequate technical and organizational measures to ensure a level of security appropriate to the risk of processing, which led to the disclosure and unauthorized access to personal data of a number of approximately 1091 data subjects who had placed orders on the controller's website. Also, the controller was sanctioned with a reprimand because did not notify the Romanian Data Protection Authority about the data breach. At the same time, a corrective measure was applied to review and update the technical and organizational measures implemented as a result of the risk assessment for the rights and freedoms of individuals, so as to avoid similar incidents of unauthorized disclosure of personal data processed.

Romania

Latest sanctions imposed by the Romanian Data Protection Authority [2/2]

— Fine of 100,000 EUR applied to a Romanian banking institution for the breach of the confidentiality and security of the personal data. It was found that the controller did not respect the principle of integrity and confidentiality of personal data which lead to the unauthorized disclosure and access to certain personal data of 4 data subjects (1 client and 3 employees). The Romanian Data Protection Authority found that the controller did not take sufficient measure to ensure that any person acting under the authority of the controller (employee) and who has access to personal data process personal data only following the request of the controller.

— Reprimands applied to two Administrative-Territorial Units for the General Directorate of Local Police for the violation of the data protection legislation. The Romanian Data Protection Authority found that the General Directorate of Local Police processes personal data through portable audio-video surveillance means of "BADGE" type, used by the staff of the Directorate in missions and activities carried out in the field, in the context in which the local police officers were hierarchically established the obligation to carry on them, during the working hours, these means of audio-video surveillance. At the time of the investigation, it was found that there are no legal provisions governing the use of portable audio-video surveillance systems in the activity of local police officers. As such, it was found that the processing of personal data (image, voice) was carried out without meeting the conditions of legality of the processing. The Romanian Data Protection Authority also applied the corrective measure to ensure the compliance of the processing operations performed by using the means of audio-video surveillance of "BADGE" type with the provisions of GDPR.

— Fine of 1,000 EUR applied to a controller for the failure to implement sufficient technical and organizational measures to ensure the confidentiality of personal data, which led to the disclosure of the e-mail address of a number of 295 data subjects. The Romanian Data Protection Authority also applied a corrective measure to ensure the compliance of personal data processing activities with the GDPR by implementing appropriate technical and organizational measures in case of remote transmissions of personal data, including in terms of regular training of persons acting under the authority of the controller (employees or collaborators).

— Fine of 3,000 EUR applied to a Romanian banking institution for the processing personal data after the end of the contractual period. The Romanian Data Protection Authority found that, due to a system error, the request of the data subject to close the current bank account did not have the effect of closing the business relationship with the controller and the controller sent to data subject messages regarding the updating of the personal data.

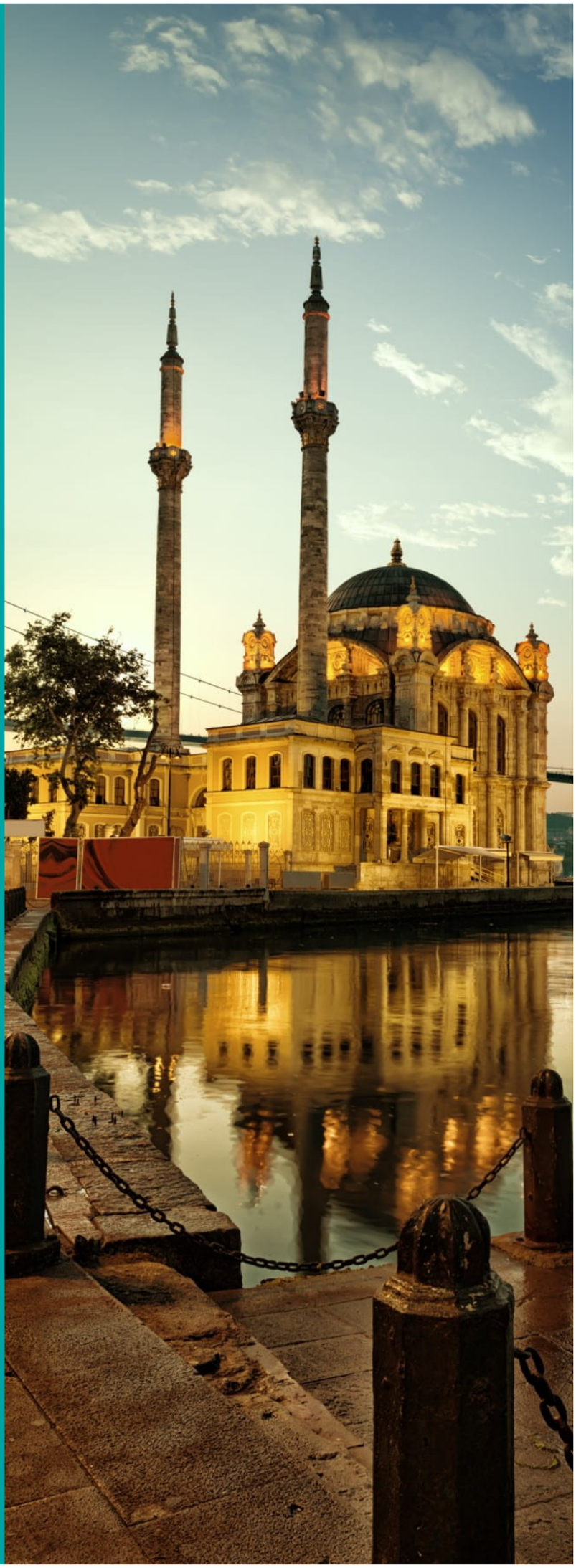
Romania

If you have any questions, please let us know

Cristiana Fernbach
Partner
KPMG Legal
T: +40 722 779 893
E: cfernbach@kpmg.com

Flavius Florea
Senior Managing Associate
KPMG Legal
T: +40 724 301 900
E: fflorea@kpmg.com

Turkey



The Spanish Data Protection and Digital Rights Guarantee Act

The Turkish Personal Data Protection Board ("Turkish DPA") published various public announcements.

Public Announcement Regarding Data Transfer Abroad

The Turkish DPA stated that it does not aim to prevent the cross-border transfers that are increasing day by day as a result of globalization and technological developments but that it aims to establish a predictable and transparent data transfer regime based on the protection of fundamental rights and freedoms. Data transfer abroad has been an issue occupying the agenda of data protection rights in Turkey. With this public announcement, the Turkish DPA underlined that it aimed to prevent misunderstandings by revealing the work and perspective of the Turkish DPA in terms of transferring personal data abroad.

In summary, considering the Article 9 of the Law on Protection of Personal Data, although transfer of personal data is possible with the explicit consent of the data subject or by way of Binding Corporate Rules, the assessment regarding the transfer of personal data abroad via adequate countries determined by the Turkish DPA remains unconcluded.

The reciprocity principle is a prior condition in the assessment of adequate countries. The Turkish DPA shall seek adequate protection for transferring data between Turkey and the countries concerned. It is also emphasized that the issue of reciprocity and the negotiations to be conducted must be based on mutual competence. In the announcement, it was stated that a unilateral recognition could create asymmetry, hence, being a disadvantage for data controllers operating in Turkey. In this context, it was stated that the studies regarding the determination of adequate country status were carried out in close cooperation with the Ministry of Justice, the Ministry of Foreign Affairs and the Ministry of Trade.

It is possible to state that an adequate country list is yet to be announced by the Turkish DPA.

Public Announcement Regarding Information Revealed to the Public by the Data Subject Herself/Himself ("Publicizing")

According to the announcement, the Turkish DPA states that the expression "Publicizing" in the Law has a narrower meaning than the public disclosure of personal data in any way; It has been underlined that the person concerned should have the will and purpose of publicizing. Accordingly, it is not sufficient that the personal data of the person is in a place where everyone can see it or that it is open to everyone. This process should also be supported by the will of the person concerned. In cases where personal data are disclosed to the public for a specific reason other than the will of the person, it will not be possible to speak of a publicization under the Law. For instance, processing a phone number shared by the data subject on a public platform for the sheer purpose of selling a vehicle, and using it for advertising / marketing purposes would be against the Law.

Decisions Published by the Turkish DPA

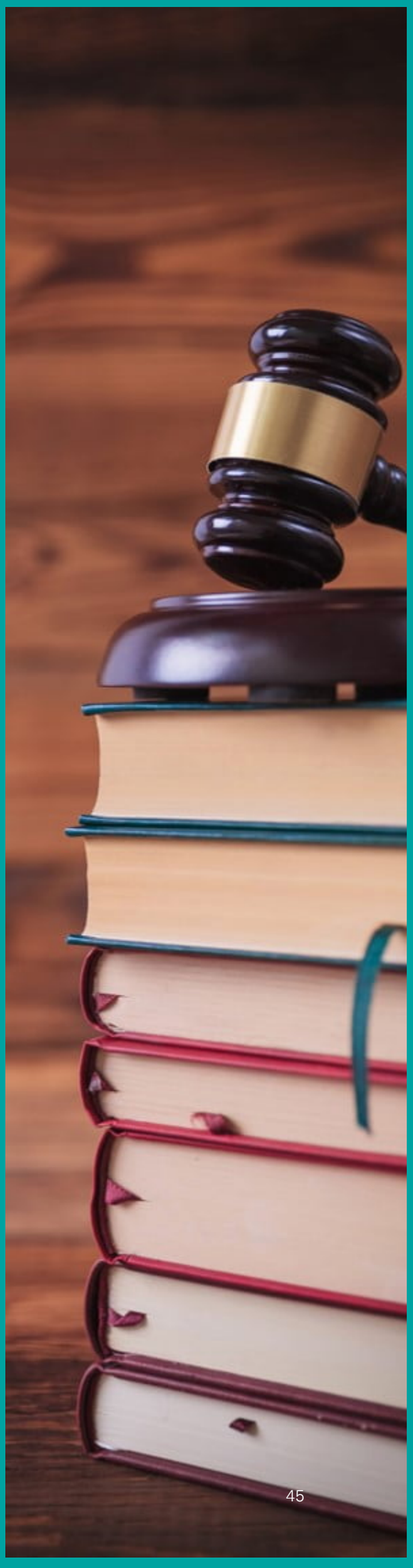
The Turkish DPA published various public decisions regarding the protection of personal data.

Decision on The Use of Biometric Signature Data

According to the announcement the Turkish DPA has determined that;

- A biometric signature is biometric data,
- The processing of data of this nature is only possible with the fulfillment of the conditions stipulated in the law or the explicit consent of the data subjects,
- That the Turkish Law of Obligations provisions do not correspond to the "conditions stipulated in the law".

Accordingly, the said processing is only possible on the condition that obligation to inform is fulfilled and explicit consent has been obtained from the relevant data subjects and the "Adequate Precautions To Be Taken By Data Controllers In The Processing Of Special Categories of Personal Data" determined by the Turkish DPA are taken into consideration.

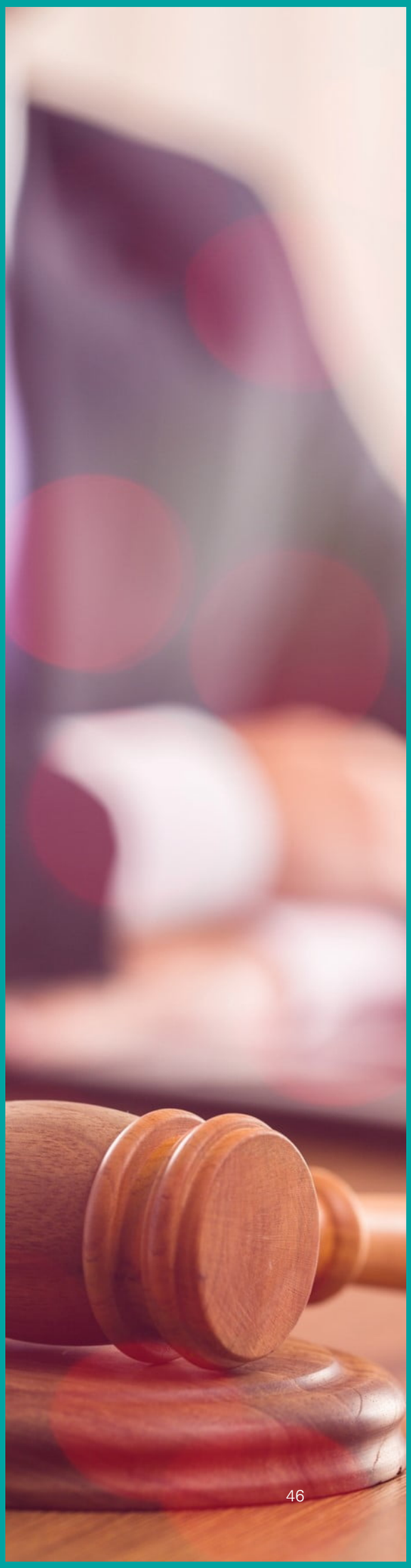


Administrative Fine Decisions by the Turkish DPA

Administrative Fine imposed on a Bank in Turkey

The Turkish DPA recently announced an administrative fine imposed on a Turkish bank, due to its failure to comply with its obligation to inform. According to the announcement the Turkish DPA examined the said bank's privacy policy due to a complaint form a data subject and had instructed the bank to correct the deficiencies determined in their privacy policy. In its defense, the bank claimed that it had fulfilled its obligation to inform in full. However, the Turkish DPA stated that no supporting documentation was presented by the bank.

The Turkish DPA concluded that the data controller bank acted against the Law and decided to impose an administrative fine of TL 120,000.



Turkey

If you have any questions, please let us know

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

United Kingdom

UK

A. What the EU-UK Trade Agreement means for data protection

B. KPMG Schrems II Solution and Supporting App

United Kingdom

What the EU-UK Trade Agreement means for data protection [1/2]

The European Union (EU) and the United Kingdom (UK) came to an agreement on December 24th, 2020.

The European Union (EU) and the United Kingdom (UK) came to an agreement on December 24th, 2020. The EU-UK Trade and Cooperation Agreement ("Trade Agreement"), is set out to define new rules from 1 January 2021. In terms of data protection, the main aspects contained in the Trade Agreement are as follows:

There is interim provision for transmission of personal data from the EU to the UK which means that the UK is not considered a third country, but this is subject to the condition that UK DP law remains as at 31 December 2020, and the UK does not exercise any "designated power" without EU agreement. These designated powers include introducing new standard/model clauses, new codes of conduct and certification mechanisms, or new binding corporate rules.

This interim period applies until there is an adequacy decision, subject to a maximum period of 4 months, which can be extended by a further 2 months unless either the UK or the EU objects (not just the automatic 6 months maximum that some media refers to).

The above will also apply to transfers to the UK from Iceland, Liechtenstein or Norway.

Throughout the document, there are also numerous references to the commitment of both parties to ensuring the correct protection of individuals' personal data. In this regard, the Law Enforcement & Judicial Co-operation section of the Trade Agreement can be suspended if there are serious deficiencies in data protection including if any future adequacy decision is revoked.

What the EU-UK Trade Agreement means for data protection [2/2]

Additional Brexit implications

Besides the points above, there are a number of aspects that have already been impacted since January 1st as a result of Brexit:

1. European Representatives. As the UK is no longer in the EU:

Under GDPR, UK organisations targeting EU individuals need to appoint a representative located in one of the EU Member States.

Global organisations with their current European representative located in the UK need to appoint a representative in another EU Member State after Brexit.

2. Regulators & One-Stop-Shop. EU's One-Stop-Shop mechanism allows international organisations to deal with a single Data Projection Authority (DPA) for cross-border matters and, as a result of Brexit, the ICO is no longer one of the EU DPAs eligible to be a regulator for EU cross-border matters. Therefore, organisations operating in both the EU and the UK will have at least two regulators (the UK ICO and the corresponding EU authority) to report to.

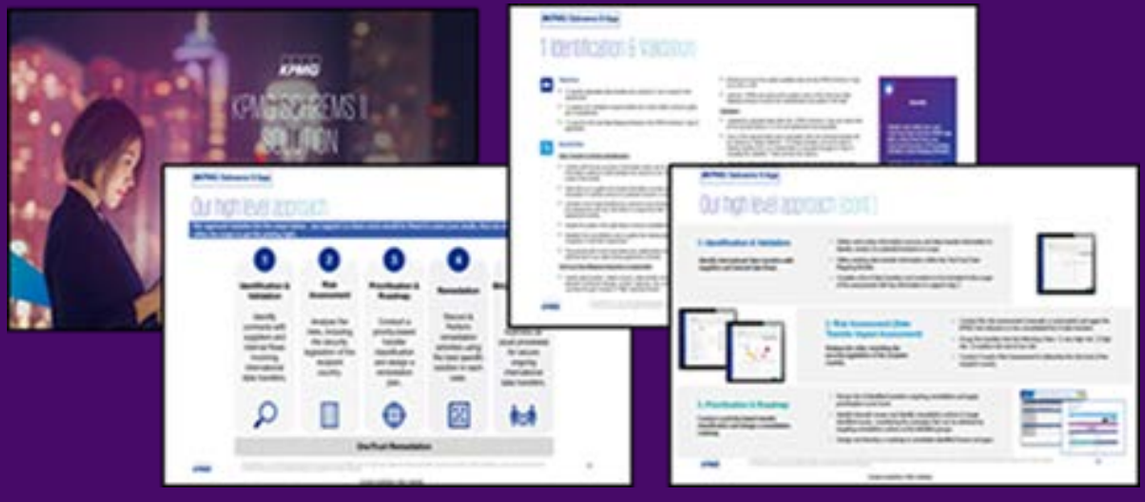
3. Accountability. Having a new legal framework in place will mean that existing privacy policies and compliance activities will need to be reviewed, and data protection impact assessments relating to cross-border issues may need to be updated.

KPMG Schrems II Solution and Supporting App

We have built an end to end Schrems II Solution and supporting App to help organizations to identify and evaluate their exposure in relation to the latest requirements on international data transfers coming from the Schrems II Judgment.

This solution provides:
End to end overview of the journey our clients need to undertake. This is significant and there is a substantial amount of advisory and legal support which our clients need.
A template proposal.
A Schrems II application which is stand-alone but also integrates with OneTrust.

As part of the above solution, KPMG is working to build a tool which risk assesses clients' international transfers (data transfer impact assessments) with the click of a button. The tool will help clients to Identify, Assess, Prioritize and Remediate data transfers using the risk assessment methodology developed by KPMG Law on the basis of the Judgment of the EU Court of Justice and the guidance of the European Data Protection Board on international data transfers. KPMG is also working with OneTrust to ensure integration for those clients who already use OneTrust as their main privacy compliance tool.



KPMG Schrems II Solution and Supporting App

Key points to note:

- We are currently building a baseline proposal deck which can be used to showcase our tool and approach with clients.
- There will be internal Global workshops planned where we will explain the service offering in more detail and the indicative pricing.
- The tool is due to be released Mid-Jan 2021.
- The tool will be low cost which will enable you to wrap around the KPMG services (per the above) to make a really compelling differentiated offering.

OneTrust and KPMG will be marketing this together in January so it is key that we engage strongly with the OneTrust Country Contacts.

United Kingdom

If you have any questions, please let us know

Isabel Ost
Director
KPMG Law UK
T: +44 207 6943361
E: isabel.ost@kpmg.co.uk

Jose Caballero
Manager
KPMG Law UK
T: +44 203 0783794
E: jose.caballero@kpmg.co.uk

Vietnam

A. Update on legal requirements for data localization in Vietnam

Update on legal requirements for data localization in Vietnam

In our previous article from the Data Privacy Newsletter dated July-August 2019, we highlighted the data localization measures in the Law on Cybersecurity (CSL) that came into effect on 1 January 2019. By way of recap, the CSL provided that both domestic and foreign enterprises providing telecommunications, internet or value-added services in the Vietnamese cyberspace must locally store user data and other sensitive information related to national security. The law also requires foreign companies to establish a branch or representative office in Vietnam, presumably to facilitate enforcement of any breaches of the law. The provisions were couched in broad language such that corporations with economic presence and business interest albeit without physical presence are captured within the ambit of this law.

Ideally, following the passage of a new law, the Vietnamese government will create and issue the implementation guidelines before the law comes into effect. However, at the time of writing, the decree regulating data localization submitted by the data regularly authority (i.e. Ministry of Public Security) has not yet been promulgated and is currently under review by the government. As such, we have used drafts to infer the intention of the authorities.

In the second draft of the decree guiding the CSL, companies, either incorporated in Vietnam or overseas, must store the data and establish a branch or representative office in Vietnam if having ALL the below:

a) providing telecommunications, internet and cyberspace-based services in Vietnam;

b) having activities of collection, exploitation, analysis and processing of the data on personal information, data produced by users in Vietnam or data on relationships of service users in Vietnam;

c) having users perform prohibited acts such as cyberattack, distributing propaganda against the State of the Socialist Republic of Vietnam, discriminating by gender and race, posting or transmitting false information etc.; and

d) resisting to the cybersecurity protection activities conducted by competent authorities; failing to comply with the requirements stipulated by the CSL on (i) user information verification, protection and provision upon the request of the competent authorities, (ii) sharing prevention and deletion of violating information within 24 hours from the competent authorities' request.

The draft decree also makes clear that the Ministry of Public Security is the authority to impose the mandate for data localization and branch/representative office incorporation on companies having all the conditions above. It would appear that such obligation would only arise once there is a request received from the Ministry of Public Security. The above regulations, if approved and passed by the Government of Vietnam, will essentially narrow down the number of companies that will be impacted by the data localization requirement, which acts as a reprieve to foreign companies with economic or business interest in Vietnam.

Although the Ministry of Public Security intends to narrow the data localization criteria, it retains discretion regarding whether a crime has been committed, leaving companies with limited ability to contest the Government's findings or directive. Until such time the decree is finalized and adopted, there are risks that the Government may exercise its powers under the CSL to compel companies to take-down content. The Ministry of Information and Communication's website reveals that since the incorporation of the CSL, corporates including international big tech companies have complied with approximately 70% of take-down requests regarding materials relating to national security. In other words, even without a decree, corporations should be vigilant to ensure that the data stored is not used by third parties to perpetrate any of the crimes listed above.

Vietnam

If you have any questions, please let us know

Nguyen Thanh Hoa
Partner
KPMG in Vietnam
T: +84 28 38219266
E: hnguyen23@kpmg.com.vn

Vo Huong Thuy
Associate Director
KPMG in Vietnam
T: +84 28 38219266
E: thuyvo@kpmg.com.vn

Amarjit Kaur
Manager
KPMG in Vietnam
T: +84 28 38219266
E: amarjitsingh@kpmg.com.vn

kpmg.com

Designed by CREATE. | CRT115985 | June 2019