Data privacy newsletter

KPMG Global Legal Services

August-September 2020

Contents

KPMG

Introduction

Welcome to the sixth edition of the KPMG Global Legal Services newsletter on developments in the world of data protection and privacy law. KPMG firms are proud to be part of a global organization, with privacy lawyers, enabling KPMG professionals to offer an international service to clients in this area.

KPMG's global organization 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 right to be forgotten, regulatory actions and statistics, health data, Schrems II case, liability of controllers, privacy abuses, obligations of entities developing or implementing location and tracking apps in the context of COVID-19 outbreak, EDPB 's Guidelines 05/2020 on cookie consent, data breaches and privacy impact assessments.

Australia

A. Insights from Australia's new Cyber Security Strategy for 2020 and bi-annual notifiable data breach report

Australia

Insights from Australia's new Cyber Security Strategy for 2020 and bi-annual notifiable data breach report

This year has seen a number of major Australian organizations impacted by malicious cyber-attacks. The most recent bi-annual report (January-June 2020) issued by the office of Australia's Data Protection Authority, the Office of the Australian Information Commissioner (OAIC), has found that these attacks were largest cause of notifiable data breaches reported in the first half of 2020. Meanwhile the Federal Government has also released the Australian Cyber Security Strategy 2020, announcing Australia's largest ever investment in cyber security amidst clear warnings of the increased risk of cyber-attacks.

The following recent findings from the OAIC's report on notifiable data breaches provide useful insights for businesses in relation to the cause and impacts of data breaches:

- 518 breaches notified. This is up 16% for the same reporting period last year.
- Malicious or criminal attacks (including cyber incidents) remain the leading cause of data breaches, comprising 61% of notifications.
- Breaches due to ransomware are on the rise and there is growing concern that the motivation is to extract data as well as encrypt it. Many businesses are paying attackers amounts ranging from thousands to millions of dollars to recover data. However, this data may still be stolen or disclosed.
- The health sector is the highest reporting sector, with 22% of all breaches.
- Contact information is the most common type of personal information involved.

Warning of the increase in breaches due to ransomware, the OAIC is encouraging businesses to:

- comprehensively understand their data, its location and lifecycle;
- consider controls such as network segmentation, additional access controls; and
- use encryption.

Australia

Insights from Australia's new Cyber Security Strategy for 2020 and bi-annual notifiable data breach report (cont.)

The 2020 Cyber Strategy seeks to create a more secure world for Australians and businesses, ensuring cyber readiness becomes a fundamental part of everyday life. While a central part of the new Strategy is ensuring that businesses take responsibility for enabling cyber security and proactively securing their products and services, the Government has identified three pillars of action to support the Strategy aimed at Government, Business and Community. Australia's regulatory structure and infrastructure will be strengthened to enable effective response to these threats. The enhanced regulatory framework will first be delivered through:

- amendments to the Security of Critical Infrastructure Act 2018; and
- the release of a new voluntary code for businesses, the Code of Practice: Securing the Internet of Things for Consumers. This will be a principles-based guide to the use and cyber security of internet-connected devices.

The Australian Government is investing AUD$58.3 million to enhance customer engagement and $12.3 million to further develop its cyber security helpdesk for SMEs and families. This includes the improvement of the Government's online ReportCyber incident tool to provide businesses support and advice when reporting, responding and recovering from a cyber-incident.

The Australian Government also plans to consult with Australian businesses on:

- privacy, consumer and data protection laws;
- duties for company directors and other business entities; and
- obligations on manufacturers of internet-connected devices.

With other reforms already being planned to the Privacy Act 1988 (Cth), the economic and social impacts of the COVID-19 pandemic, and new rules for data sovereignty being considered, a focus on cyber related privacy and data legislative reform for both critical and non-critical business to manage cyber risks. It is a further opportunity to consider the effectiveness of current laws and how data protection represents a new focus for the data protection and privacy is managed in Australia.

Australia

If you have any questions, please let us know

Veronica Scott
Director
KPMG Law Australia
T: +61 (0)3 92885787
E: vscott1@kpmg.com.au

Kate Marshall
Partner and Head of KPMG Law
KPMG Law Australia
T: +61 (0)3 92885787
E: kmarshall@kpmg.com.au

Belgium

A. Belgian DPA sanctions violation of right to be forgotten

B. Belgian DPA issues further guidance on body temperature testing

Belgium

Belgian DPA sanctions violation of right to be forgotten

On 14 July 2020, the Belgian Data Protection Authority (BDPA) issued a fine of 600.000 EUR regarding a violation of a data subject's 'right to be forgotten'.

The investigation of the BDPA was initiated following a complaint filed by a data subject whose request to have certain online search results delisted was refused. In its decision the BDPA provided some valuable insights on the right to be forgotten.

After having confirmed its territorial authority, the BDPA examined the request of delisting in detail.

The data subject was a public figure whose delisting request consisted out of a number of search results relating to a) his relationship with a political party and b) a complaint filed against the data subject for "bullying" (over 10 years ago).

The BDPA examined in detail the separate requests and the search results. In its decision the BDPA made a clear distinction between both categories of search results.

As the data subject, according to the BDPA's decision, exercised a public function, the results relating to his relationship with a political party were considered to be relevant for the public interest and thus the right to be forgotten could not be applied here.

On the other hand, the second category of search results was no longer considered to be relevant, amongst others because the bullying complaint was found to be unsubstantiated in 2010 and the data subject had provided sufficient proof in this respect.

For the second category of search results, the BDPA thus considered that the right to be forgotten was violated. In its decision, the BDPA took into consideration that the motivation to retain the search results (following the data subject's request) was clearly insufficient.

Apart from the fine, the BDPA also stated in its decision that the electronic forms for the filing of a request should be modified and made more transparent.

Belgium

Belgian DPA issues further guidance on body temperature testing

On 5 June 2020 the Belgian Data Protection Authority (BDPA) published new updated guidelines regarding the measuring of the body temperature of data subjects.

In its guidance the BDPA makes the following distinction to clarify if the measuring of body temperature falls within the scope of the GDPR.

1. Mere reading of the body temperature without any recording of the temperature

The mere reading of the body temperature on a classic thermometer without recording this in a file will not be considered as an activity involving the processing of personal data and falls outside the scope of the GDPR. Also, the consequences that are associated with the (level of) body temperature (i.e. refusing access to the premises due to (1) a high temperature (i.e. fever) or (2) the refusal of a temperature check by the data subject) fall outside the scope of the GDPR under the condition that no additional registration of personal data has taken place.

2. Reading of the body temperature including the recording of the temperature in a file

When the body temperature of a data subject is recorded in a file, this recording will be considered as an activity involving the processing of personal data (i.e. health data) and falls within the scope of the GDPR. Therefore, the recording of the body temperature of a student or an employee in his/her student/personnel file is forbidden since no lawful processing ground is currently available.

3. Advanced electronic measuring techniques of the body temperature

Moreover, the GDPR is not only applicable when personal data is being recorded but also if the processing of personal data takes place in an advanced digital manner, which is the case when automatic (or remote) means are being used. The GDPR states that processing means "any operation or set of operations which is performed on personal data or on sets of personal data whether or not by automated means". Therefore, advanced digital thermometers, heat scanners or other automatic means that measure the body temperature of a data subject are considered to be an activity involving the processing of personal data, in particular health data, and are consequently prohibited.

Belgium

Belgian DPA issues further guidance on body temperature testing (cont.)

Conclusion

To conclude, the BDPA has stated that the mere reading of the body temperature falls outside the scope of the GDPR, under the condition that the body temperature and consequences are not being recorded. However, as soon as there is a (i) recording in a file or (ii) a fully or partially processing operation by automated means of the body temperature, the GDPR does apply and the data controller needs to respect all principles of the GDPR (i.e. lawfulness, transparency, data minimization, etc.).

The BDPA clearly states that consent will, in most cases, not be considered to be an appropriate legal ground for the processing of the body temperature, since this consent will not be freely given especially in a labor context. Since there is currently no specific and clear lawful basis to process the health data (by a law or collective labor agreement), data controllers are not allowed to:

- record the body temperature of the data subject in a file;
- record the consequences related to the body temperature of the data subject in a file (i.e. for example no access to the building); or
- record the body temperature via advanced electronic devices such as: an advanced digital thermometer, heat scanner or other automatic means that measure the body temperature.

The above guidelines remain subject to future modifications and amendments by the BDPA.

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

Bulgaria

A. Organizing Group Testing of Employees for Covid-19

B. Processing Health Data of Employees Working from Home

Bulgaria

Organizing Group Testing of Employees for Covid-19

Bulgarian Data Protection Authority (BDPA) state that an employer may rely on its legitimate interest as a legal ground for processing data in order to organize group testing of employees, if the balancing test shows that employer's interest prevail.

BDPA was asked to provide guidance on employers' possibilities to process employee's personal data for the purposes of group PCR-testing for Covid-19 in compliance with GDPR.

The BDPA held that since Bulgarian legislation does not provide for obligations for employers to perform tests and process health data, employers are only allowed to organize tests. According to the BDPA, employers do not have legitimate need to process any health related data, including genetic data contained in the PCR-test samples.

An employer, led by its legitimate interest to ensure business continuity, may undertake measures to preserve employees' health in the epidemic crisis situation by organizing their group testing.

An employer may only process health data at a later stage, if and when an employee submits a sick leave note to certify that he/she was treated for Covid-19. Until that moment, the employer does not need and is therefore not entitled to process employees' health data.

Bulgaria

Processing Health Data of Employees Working from Home

The Bulgarian Data Protection Authority (BDPA) state that employers are generally not allowed to collect health data from employees working from home. Employers may inform the personnel that there is a sick employee without identification.

The BDPA was referred to rule on whether employers are allowed to require employees who work from home to provide information on whether they or their family members suffer from Covid-19, as well as if they undergo quarantine measures under suspicion of contagion.

The BDPA held that since the matter refers to the health condition of employees who work from home, employers' supervision cannot be spread over home and family lives of employees. In this regard, there is no applicable legal ground for the employer to require any such information from employees, due to the fact that these employees are isolated and do not pose a threat to their colleagues' health. The BDPA adds that other facts such as work regime and meetings between employees must be taken into account.

It is underlined that information concerning health of employees who work from home may be processed when that information has been made publicly available by the data subject (Art. 9, para. 2, item "e" of the Regulation), as well as in cases where the employee submits a sick leave note to certify that he/she is treated for Covid-19. Information on household members being ill may be processed, if any such information is contained in the sick leave note. Until such event, the employer does not need to process health data on individuals working from home.

According to the statement, the employer may provide information to other employees about one of their colleagues being ill, if this is positively confirmed, but without providing data to identify the individual, i.e. without reference to his/her name.

Bulgaria

If you have any questions, please let us know

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

Siana Garbolino
Senior Manager, Legal Advisory
KPMG in Bulgaria
M: +35929697600
E: sgarbolino@kpmg.com

Teodor Mihalev
Lawyer, Legal Advisory
KPMG in Bulgaria
M: +35929697600
E: tmihalev@kpmg.com

Czech Republic

A. More than 100 data breaches in less than 6 months

B. Inspection results for the first half of 2020

C. The Czech Data Protection Authority commented on the Schrems II case

D. Liability of controllers for external information systems

Czech Republic

More than 100 data breaches in less than 6 months

The Czech Data Protection Authority dealt with more than one hundred cases of notified breaches of personal data security in the first half of 2020 – most of the breaches were targeting financial institutions, hospitals and municipalities.

Among the most frequently used attacks were phishing attempts targeting information systems of various subjects, including the systems of major Czech hospitals. The danger of this attack lies in losing access to the information systems which in the case of hospitals could turn out to be a devastating problem. Being exposed to such a threat, the hospitals have been forced to implement stricter backup and security policies.

Another example of data breaches, although less serious than the previous one, is of a high school student that hacked the school system (probably by figuring out his teacher's weak login details) to change some of his grades and improve his attendance.

A common trend of these data breaches is that controllers often times do not operate systematically when it comes to data protection. The data breaches are usually caused by inadequate training of employees, overlooking safe practices for personal data protection and underestimating password protection policies. Following only the basic principles for data protection is insufficient.

It is also worth noting that the blame can never fall solely on the employee that caused the data breach. The personal data controller is always responsible for data protection as a whole.

On the bright side, the notifiers almost always rectified their mistakes and took remedial actions. To this end, the remedy should consist not only of problem solving but also of prevention, such as proper retraining of employees for dealing with personal data.

Inspection results for the first half of 2020

The Czech Data Protection Authority (CDPA) has published an overview of resolved inspections for the first half of 2020 on its website. The inspections covered various areas and topics.

For example, in the area of employment a complaint was lodged for using an attendance system with fingerprint recognition technology and also for tracking employees via a camera system when working with a computer. In particular, the complainant questioned the lawfulness of such processing, the lack of information provided and the security of personal data. The employer processed personal data on the basis of consent granted by the employees, however, the consent did not meet the legal requirements set forth by GDPR, since the information about the purpose, methods and time of processing of the biometric data (fingerprints) were not clearly formulated and lacked transparency. During the inspection, deficiencies were rectified by the controller.

In another case, an inspection was initiated against the copying of personal ID documents of clients as part of business activities when renting sports equipment. The complainant stated that he had not been sufficiently informed as to why his personal ID document was copied and how his personal data were handled.

The CDPA assessed that the scanning of ID cards was not lawful. Furthermore, the controller did not credibly explain the scope of processed personal data. Namely, in some cases personal data of a special category were processed. The inspection will be followed by the procedure for imposing a fine.

Another complainant had been contacted via telephone by a representative with an offer of services. During the call, he was directly addressed by his surname, from which it was clear that the controlled company processed not only his telephone number, but also other personal data. Furthermore, it was discovered that the controller processed the personal data of clients who agreed to the processing only orally – by telephone, and this fact was not recorded or archived in any way. It was concluded that the abovementioned procedure was inadmissible. The inspection was followed by an administrative procedure on the elimination of deficiencies.

Czech Republic

The Czech Data Protection Authority commented on the Schrems II case

As is already known, the Court of Justice of the EU (CJEU) invalidated the Privacy Shield, based on which it was possible to transfer personal data to the US, and left standard contractual clauses in effect under certain conditions.

The Czech Data Protection Authority (CDPA) concluded that the CJEU decision includes recommendations for personal data controllers on how to deal with the situation. Any controller transferring personal data to the US on the basis of standard contractual clauses should seek and propose solutions in the form of additional security safeguards (e.g. data storage including metadata only in the EU).

The CDPA pointed out that if processors, as importers of data, are subject to US law, the risks arising not only from the CJEU decision but also from the so-called CLOUD Act need to be assessed separately. The controller may only use a processor that provides sufficient guarantees of the implementation of appropriate technical and organizational measures.

At the same time, the controller should not forget the principle of transparency and inform the data subject about specific measures and procedures to whom and to which countries the data are made available / transferred, under what conditions, how the data are protected, or related risks.

Czech Republic

Liability of controllers for external information systems

The message of the Czech Data Protection Authority (CDPA) is simple – having information systems created by an external contractor does not relieve the data controller from the responsibility for any personal data processing that takes place in such systems.

In accordance with the GDPR, it is always the personal data controller who is responsible for the entire processing of personal data. That applies even if the data controller hired an external supplier to provide an information system. Moreover, controllers have to ensure and be able to prove that personal data are being lawfully processed. Therefore, controllers cannot argue that they are using an external contractor's information system and that some functionalities are given by the default system settings.

This can be demonstrated in the case of a public university that hired an external contractor to make a system for handling student applications. The system required students to use their national identification number for logging in. Such use was in violation with the respective Czech laws and the purpose of the processing was also not legitimate. The university argued that it could not influence the privacy measures of the system and its settings. This argumentation was refused by the CDPA.

The data controller is supposed to consider the functionalities and settings of the system in light of the privacy by default and privacy by design principles. The CDPA suggests that controllers should cooperate with external providers from the very beginning to ensure that the completed system serves the needs of the controller and at the same time complies with personal data protection requirements. At the same time, the usage of the information system, even if the same system is used by different controllers, must be always assessed individually in light of the particular circumstances.

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. The Intellectual Property Report of KPMG Law 2020/21

B. German data protection authorities publish guidance on Art 15 para 3 GDPR

C. Federal Cartel Office may prohibit processing of Off-Facebook data

D. Fine of 1.24 mln. EUR against a German statutory health insurance

E. Draft of a uniform data protection law for the telecommunications and telemedia sector

The Intellectual Property Report of KPMG Law 2020/21

For the fifth time, the Intellectual Property Survey of KPMG Law 2020/21 is addressing globally operating companies active in the patent and trademark business. Once more, it will deliver a valuable and profound insight into the daily challenges and measures for optimization. It will provide trends, strategies and KPIs – such as performance and cost-KPIs – for the precise benchmarking of IP Departments in an International framework.

"Data protection/data security" was named by European IP departments as one of the top 3 most important challenge for 2018/19, together with the "provision of proactive advising" and "optimization of work processes/procedures". It comes as no surprise that the intellectual property departments are no exception to the increasing importance of data protection. These mentions by heads of IP provide a clear signal that visibility and reputation, issues related to data protection and work optimization strategies will dominate the work of the IP department in years to come.

The Intellectual Property Survey of KPMG Law 2020/21 is dedicated to questions like these. In light of today's fast-changing and complex business environment, innovative ideas are of increasing advantage for competitive businesses. Intellectual property is therefore of incredible value in order to maintain a thriving business. In consequence, it is crucial to consider best practices of daily challenges such as staffing, cost reduction and outsourcing practices when it comes to the organization of an IP department.

This global benchmarking initiative will provide valuable insights into the most crucial aspects of managing an efficient and modern IP department. Questions regarding the organization of the IP work, activities in the IP department, cooperation with law firms and current developments and trends in the IP department will be evaluated. The questionnaire has been developed in cooperation with an Advisory Board of 14 IP-experts of well-known international companies in order to guarantee the relevance and accuracy of the results.

Not only will this evaluation allow us to benchmark any organization in relation to other survey participants on numerous aspects of the IP department, it will furthermore enable us to determine future strategies and adjust organizations and processes in the most efficient manner.

Germany

German data protection authorities publish guidance on Art 15 para 3 GDPR

In their yearly activity reports, some of the German data protection authorities (GDPA's) have dealt with the scope of the claim to copies of personal data according to Art. 15 para. 3 GDPR. Most of the authorities have taken a rather restrictive approach on the amount of data to be handed out.

While most of the GDPA's are of the opinion that there is initially a comprehensive right to information and copies, they also contest that there is ultimately no general right to the surrender of documents, files or e-mails containing information about the person concerned. According to the GDPA's, the companies only need to deliver a structured summary of the personal data required so that the data subject can check the accuracy of this data and the lawfulness of the processing.

The full release of copies of all documents with information about the person concerned is regularly in conflict with the rights and freedoms of other people. In addition, a comprehensive release would reveal internal processes, trade secrets or other know-how. However, the GDPA's also acknowledge that it may also be necessary to hand over copies of individual documents in certain cases.

The German courts have so far taken a very diverse stand on the question of the scope of the claim to copies. While some courts have taken a rather restrictive stand, some courts have granted the demand for a full copy of all information in question.

In light of this ambiguity, some of the GDPA's have expressed a strong desire for a clarification by the legislative.

Federal Cartel Office may prohibit processing of Off-Facebook data

The Federal Cartel Office accuses Facebook to abuse its dominant market position by forcing its users to consent to the processing of their Off-Facebook data. This lawsuit was the first in Germany to raise the question as to the conditions under which a privacy infringement may constitute an antitrust violation. While the final decision is pending, the German Federal Court of Justice (Bundesgerichtshof), by order of 23 June 2020, decided that the Federal Cartel Office indeed has the power to prohibit the Off-Facebook data processing – at least for the time being.

What has happened?

According to its terms of use, Facebook collects and processes not only personal data its users share deliberately, but also data that is collected based on their habits on linked websites and related platforms, such as Instagram or WhatsApp, as Off-Facebook data. Every consumer willing to join the social media platform must consent to his or her data, within and off the network, being compiled and processed by Facebook. By aggregating the collected personal data, Facebook generates user profiles and displays personalized advertising in order to finance the free of charge platform.

By order of 6 February 2019 , the German Federal Cartel Office assessed this conduct as a data protection infringement as well as an antitrust violation and forced Facebook to stop this practice.

The authority voiced the opinion that Facebook abuses its dominant market position by demanding consent to these terms of use in breach of the GDPR without giving end-user any choice other than not to use Facebook at all.

In response, Facebook filed a complaint with the Higher Regional Court Düsseldorf in an injunctive process with the aim to render this prohibition unenforceable. While the judgment in the main proceeding is still pending, the court granted Facebook's request and decided that the prohibition should be unenforceable until a final decision. The German Federal Court of Justice, in turn, annulled this interim decision to the effect that the German Federal Cartel Office's prohibition of the use of the terms is enforceable again.

What is at issue?

These proceedings and the increasing economic importance of data have brought to focus the question, in which cases a privacy infringement may also constitute an antitrust violation.

The Federal Cartel Office accuses Facebook, inter alia, to processing Off-Facebook data unlawfully. It points out that there is no legal basis for data processing, neither consent nor any statutory basis in the GDPR. Persuant to the GDPR, consent is only valid if it is given voluntarily without any compulsion. According to the Cartel Office, Facebook has a quasi-monopolistic position on the market for social networks that creates a clear imbalance between the network and its users.

Federal Cartel Office may prohibit processing of Off-Facebook data (cont.)

It says that by making the consent conditional on the terms of use to the registration, Facebook refused its users a genuine or free choice to consent. Otherwise the access to the dominant network would be denied. As per the Cartel Office, this infringement of data protection by a dominant company must also be regarded to be anti-competitive as a result – and therefore constitutes an antitrust violation.

The Higher Regional Court Düsseldorf, on the other hand, is of the opinion that the consent is freely given. It claims that every consumer had the free choice whether to join Facebook and allow the processing of personal data or forego the use of this social media. This decision was the result of a personal benefit-risk-assessment. In the court's view, a compulsion to consent does not exist. Furthermore, causality in relation to the outcome could not be considered as a sufficient condition for an antitrust violation. According to the court, a violation of antitrust law would assume strict causality of market power, requiring proof that data processing conditions could be used in such a way precisely and solely because of market power. Such a causality had not been alleged by the Federal Cartel Office. So even if there was an infringement of data protection, pursuant to the Higher Regional Court Düsseldorf, this could not constitute an antitrust violation.

However, the Federal Court of Justice overruled this order and argued that there aren't any serious doubts either about Facebook´s dominant position in the German social network market or its abuse.

By refusing the consumer any choice on what to consent to, Facebook affected the users right of privacy and violated antitrust law. Due to the "lock-in-effect", created by the barriers that prevent users from switching to competitors, the market was no longer able to control the competition effectively.

In addition, these terms of use are likely to interfere with free competition and may cause a negative impact on the online advertising market.

What are the consequences?

While the Higher Regional Court Düsseldorf upheld the test of strict causality to establish an antitrust violation by privacy infringements, the Federal Court of Justice indicated a less restrictive view on this causality.

However, both rulings by the courts were thus far only preliminary decisions in injunctive proceedings. Therefore, the impacts of this ruling on the final decision remain to be seen. But with the courts and the Federal Cartel Office being bound by the ruling of the Federal Court of Justice, even this preliminary decision may be a game changer for the question of how far user consent may be stretched before facing antitrust issues.

In addition, the final decision will most likely be a litmus test on the questions whether any processing of personal data by monopolistic companies can be regarded as an anti-trust violation if and when the processing is not in accordance with the GDPR.

Germany

Fine of 1.24 mln. EUR against a German statutory health insurance

The State Commissioner for Data Protection and Freedom of Information for the German federal state Baden-Württemberg (LfDI) imposed a fine in the amount of EUR 1,24 mln. on a German statutory health insurance for violating data protection law.

Background

In the years 2015 to 2019 the fined German statutory health insurance organized raffles. During those raffles the statutory health insurance collected inter alia the contact details of the participants and their information about their health insurance. The statutory health insurance intended to use the contact information also for advertising purposes, but only if the participants had given their consent. However, more than 500 participants were contacted although they had not given their consent for their contact details being used for advertising purposes.

The reason for the failure was that the technical measures and the internal guidelines and training at the statutory health insurance were not sufficient to prevent the wrong participants from being written to. As a result, the statutory health insurance immediately stopped its sales activities with the data collected in raffles and announced that it will work closely with the Data Protection Authority LfDI. It also set up a task force for data protection and reviewed its consent forms and adapted other internal processes and control structures.

Assessment of the fine

The fine of 1.24 mln. EUR appears to be considerably high at first given the facts of the case, but according to the LfDI the fine could have been even higher. The fact that the statutory health insurance carried out comprehensive internal reviews and adjustments of its technical and organizational measures and of course the constructive cooperation with the LfDI during the investigation had a positive effect on the amount of the fine.

Germany

Fine of 1.24 mln. EUR against a German statutory health insurance (cont.)

In determining the amount of the fine, the LfDI also considered the following criteria set out in Article 83 GDPR: status and public task of the statutory health insurance and its importance for the German public health system, size and number of insured people. Fines under the GDPR, on the other hand, should not only be effective and dissuasive, but also reasonable. Therefore, when determining the amount of the fine, the LfDI had to ensure that the fulfilment of this statutory task was not jeopardized. The challenges of the current COVID-19 pandemic were also given special consideration.

Lessons to be learned

The case shows the clear tendency of the German data protection authorities to impose higher fines on controllers even for cases which only affect a relatively small amount of data subjects. This seems to be especially the case when the data protection violation is based on a lack of or the failure of internal technical and organizational measures. It can only be assumed that the fine would have been significantly higher if the controller was a "normal" controller and not a statutory health insurance with a decisive role during the COVID-19 pandemic.

Draft of a German "E-Privacy Act"

The Federal Government of Germany is planning a new "Act on Data Protection and the Protection of Privacy in Electronic Communications and Telemedia and on Adjusting the German Telecommunications Act, the Telemedia Act and other laws" (TTDSG).

The draft is still an unofficial document indicating that the regulations on data protection in the Telecommunications Act (TKG) and those in the Telemedia Act (TMG) are to be repealed and combined in a separate act – the TTDSG. In this process the necessary adaptations to the GDPR shall be made and the EU regulations on cookies shall be implemented in national law. In this way, an "effective and user-friendly" law shall be created.

Background of the draft law

The motivation for the revision of the data protection regulations results on the one hand from Art. 95 GDPR, according to which the implementation of the ePrivacy Directive in the German TKG is no longer in conformity with the Directive, and on the other hand from the most recent case law of the European Court of Justice regarding the use of cookies (ECJ, C-673/17).

In the introduction to the published document, it is stated that the coexistence of different laws (GDPR, TMG and TKG) leads to legal uncertainties for consumers, service providers and regulatory authorities. Therefore, it is the aim to create legal clarity for all parties concerned.

Content of the draft law

Section 3 of the draft makes provisions for the use of Personal Information Management Services (PIMS). These are systems that are used to manage employees, such as time recording systems. Users should be able to better control their personal data. PIMS must comply with certain basic standards and their use should be voluntary.

Section 9 of the draft deals with the use of cookies. The storage of information on a terminal of the end user or access to information already stored in the terminal of the end user is only permitted if the end user has been informed about it in accordance with the rules of the GDPR and has given his consent.

An exception to the obligation to give consent shall be made under the following conditions:

(1) "if it is technically necessary for the transmission of communications via an electronic communications network [...]".

(2) " if it has been expressly agreed in a contract with the end-user for the provision of specific services".

(3) "if it is necessary to comply with legal obligations.«

Draft of a German "E-Privacy Act" (cont.)

Section 14 deals with the anonymization of location data. Geo-information must be anonymized. Mobile phone users must be informed by text message that their location has been determined. If service providers process location data of users which are not necessary, for example, to forward a message via an electronic communications network, this may only be done to the extent and for as long as it is necessary to provide services with added value.

The TTDSG shall also provide strict rules against the misuse of telecommunication systems with hidden microphones and cameras, such as intelligent loudspeakers like "Alexa" or "Siri". The user must be made aware that the telecommunication system is forwarding audio or image files to the manufacturer or other companies. The user must also be able to determine what is recorded by him.

Furthermore, the TTDSG also redefines the responsibilities of the German Federal Network Agency (Bundesnetzagentur) and the German Federal Data Protection Commissioner (BfDI). The BfDI shall take over the supervision of the entire protection of personal data referring the telecommunications and telemedia sector. Until now, the German Federal Network Agency has been responsible for banning the unauthorized interception of communications and complying with information requirements.

Scope of the draft law

The draft law also stipulates for the sector of telecommunications, that the TTDSG only covers data protection in public electronic communication networks. Corporate networks and telecommunications services which are not provided via public networks fall outside the scope of the TTDSG.

Fines are aligned with the GDPR

The fines for infringements are determined by Art. 83 GDPR, according to Section 25 of the TTDSG. This means that infringements can become considerably more expensive in the telecommunications and telemedia sector.

Entry into force

The target date for the TTDSG to enter into force is 21 December 2020. Since the draft law is not yet an official document and associations still have to be consulted on the draft, it remains to be seen whether this date can be met and if the content of the new TTDSG can be adopted as drafted.

Germany

If you have any questions, please let us know

Andreas Bong
Partner, Legal Process & Technology
KPMG Law, Germany
M: +49 211 4155597-160
E: jandreasbong@kpmg-law.com

Chloé Lybaert
Associate, Legal Process & Technology
KPMG Law, Germany
M: +49 211 4155597-366
E: clybaert@kpmg-law.com

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

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

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

Dr. Ariane Loof
Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
M: +49 (0) 30 530199-625
E: aloof@kpmg-law.com

Italy

A. Local Authorities: Italian Data Protection Authority, stop illegal dissemination of personal data

B. Public Health: Italian Data Protection Authority asks for greater security of patients' personal data

C. Iliad Italia and Wind Tre fined by Italian Data Protection Authority for privacy abuses

Italy

Local Authorities: Italian Data Protection Authority, stop illegal dissemination of personal data

The Italian Data Protection Authority (IDPA) recently fined 2 Municipalities, a union of Municipalities and a Region for illegal dissemination of personal data.

Local authorities must pay particular attention to whether, on the basis of the legislation, they can publish the personal data, often particularly confidential, contained in resolutions and other documents. This was reiterated by the IDPA in some fines imposed on 2 July 2020 to a Region, two Municipalities and a Union of Municipalities.

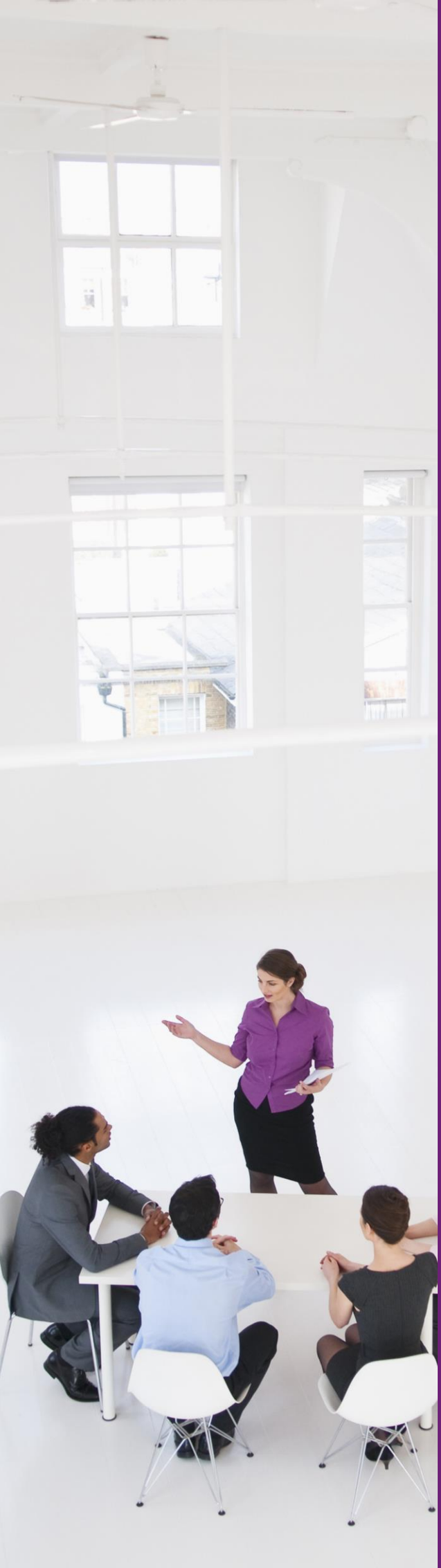
The first measure concerns a Region that had published on its website a document concerning the execution of a civil sentence relating to a debt accrued by the entity. The Region responded to the complaints of the whistleblowers by justifying the online publication on the basis of some accounting law provisions.

However, the IDPA stated that the personal data contained in those documents could rightly be used for checks by the accounting court on off-balance sheet debts, but that the aforementioned regulations and provisions did not provide any dissemination of those data.

Taking into account the collaboration offered by the local authorities and the commitment to verify the technical and organizational measures adopted by the staff for the privacy compliance, the IDPA imposed a fine of 4,000 euros on the Region.

The IDPA also fined two local authorities, a Municipality and the Municipal Union to which it belongs, which had published administrative documents of the complainant on their respective websites, in the transparent administration section or in the online register, also disseminating criminal convictions and offenses personal data. During the investigation, the two public administrations argued that publication was mandatory pursuant to the legislation on transparency of the documents and that, in any case, the person concerned was hardly identifiable, as in the published administrative documents only the serial number or the initials of the surname and name of the complainant were shown. In addition, one of the two administrations, among other things, stated that the publication had also been endorsed by the authority's Data Protection Officer. However, the IDPA noted that the aforementioned regulations did not allow the dissemination of those personal data, including those relating to criminal convictions and offenses. Furthermore, the data subject could easily be identified by colleagues, acquaintances and numerous other subjects in the local area. Therefor the Municipality and the Union of Municipalities have been fined, respectively, for 4,000 and 6,000 euros.

The latest provision concerns, instead, a Municipality that had sent by e-mail, to some local newspapers, a "citation decree" with the criminal convictions and offenses data of five people, including three witnesses cited to appear.



Italy

Local Authorities: Italian Data Protection Authority, stop illegal dissemination of personal data (cont.)

The local authority had justified the transmission of the document to journalists in order to protect its image and exercise the legitimate right of criticism against certain attacks published on the press. Also in this case, the IDPA stated that the communication of such data was not justified by the alleged "*execution of a task related to the exercise of public authority*" or by another regulatory basis, such as that on transparency. A fine of 2.000 euros was therefore imposed on the municipality.

In accordance with the abovementioned fines and provisions, the IDPA stated that the processing of personal data carried out by public entities is lawful only if necessary to fulfil a legal obligation to which the data controller is subject or to execute a task of public interest or connected to the exercise of a public authority of which the data controller is invested. The IDPA also added that the dissemination of personal data (such as publication on the Internet) by public entities is allowed only when specifically provided for by a law or regulation.

In any case, the local Authority is required to comply with the principles indicated by the GDPR, in particular, those of lawfulness, correctness and transparency as well as minimization, on the basis of which personal data must be adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed.

Italy

Public Health: Italian Data Protection Authority asks for greater security of patients' personal data

The Italian Data Protection Authority (IDPA) admonished an Italian Local Health Authority and a Polyclinic after two data breaches.

An ASL (Italian Local Health Authority) and a Polyclinic were admonished by the IDPA for two security breaches (data breaches) that had caused unlawful processing of personal health data. The incidents had been brought to the IDPA's attention by the same data controllers which, as required by EU regulations, had regularly notified the IDPA of the data breaches occurred.

The warning is one of the new powers granted by the GDPR to the Data Protection Authorities, which allows them - in the presence of a minor violation or if the pecuniary sanction to be imposed should constitute a disproportionate burden for a natural person - to detect the violation and record it in the register kept by the Authority instead of adopting a pecuniary fine. This allows the Authority, in the event of a recurrent offence, to take it into account in the quantification of the sanction.

In the case reported by the ASL, a patient who had requested a hard copy of his medical records had been given, by mistake, that of another patient, while in the case reported by the Polyclinic, a patient had found a report of another person in his or her Electronic Health Record (the so called "FSE").

In the first episode, the IDPA, with the provision of 2 July 2020, found that there had been an undue communication of health data (*i.e.* special categories of data) of a patient to a third party.

Nevertheless, considering that the documentation, as declared by the same Local Health Authority, had been returned to the hospital immediately, the IDPA qualified the case as a "minor violation" within the meaning of the EU Regulation.

The IDPA therefore admonished the Local Health Authority for the violation of the GDPR without taking any further measures, also taking into account the fact that the episode was unique and isolated, caused by a human error of enveloping, and that the Local Health Authority, as soon as it became aware of the incident, adopted corrective measures in the procedure for the preparation and delivery of medical records aimed at preventing the repetition of similar incidents in the future.

Italy

Public Health: Italian Data Protection Authority asks for greater security of patients' personal data (cont.)

With regard to the second episode, the safety violation reported to the IDPA by the Polyclinic led to the inclusion in an FSE of a report of another patient. In this case too, the confidentiality provisions relating to the disclosure of personal health data to third parties had been violated. However, having examined the circumstances of the concrete fact, the IDPA, with the measure of 9 July 2020, qualified the violation as "minor" in this case as well, deeming sufficient to admonish the Polyclinic.

In fact, the episode, unique and isolated, was caused by an unintentional human error and the healthcare facility, in addition to having informed the data subject concerned of the incident, adopted organizational measures and training initiatives aimed at raising staff awareness of compliance with data protection provisions and procedures for the correct identification of patients.

The two episodes, which are objectively limited in scope, demonstrate that staff awareness and the provision of adequate organizational measures represent, like the technical measures, are essential elements of processing activities safety.

Iliad Italia and Wind Tre fined by Italian Data Protection Authority for privacy abuses

The Italian Data Protection Authority Garante (IDPA) investigations on the telephone operator markets continued and several infringements of the GDPR committed by two of the main Italian telephone operators - Wind Tre and Iliad – have been found.

The IDPA, after numerous complaints related to marketing activities, has continued its investigation into the telephone operators market. At the end of these investigations, the IDPA issued a heavy financial penalty on Wind Tre for breaching data processing rules, with rival Iliad Italia also penalized, albeit to a much lesser degree.

Wind Tre Spa and Iliad Italia has been fined, respectively, for 16,729,600 euro and 800,000 euro for unlawful data processing.

With regard to Wind Tre Spa, the investigation of the IDPA highlighted multiple cases where complainants had been contacted by the operators by means of SMS, email, fax, phone and automated calls without having previously collected their consent. The IDPA also found cases where personal data was displayed in public directories without user consent.

It was also found that users were unable to revoke previously provided consent or to exercise their rights like to object to the processing of their personal data for marketing purposes, partially due to inaccuracies in the contact information published in the related privacy policy.

In addition, the MyWind and My3 apps were set up in a way that upon access, obliged data subjects to provide their consent for different data processing activities and purposes which included marketing, profiling, communication to third parties and glocalization, with revocation possible only after 24 hours.

Furthermore serious problems concerning the supply chain of Wind Tre's business partners were also revealed, including the improper activation of contracts. For instance, one partner of the telephone operator – which had sub-contracted out, in absence of a legal act, entire phases of processing to call centers that unlawfully collected and processed those data – was fined for 200,000 euro by the IDPA and was furthermore prohibited from using the data collected and processed in total disregard of the GDPR.

Alongside the hefty fine, Wind Tre was banned from processing data without consent, and ordered to adopt technical and organizational measures to control its partners' supply chains in order to avoid any further similar event.

With specific regard to Iliad Italia, the investigations of the IDPA found flaws in the ways employees accessed network traffic data.

If you have any questions, please let us know

Dr. Michele Giordano
Managing Partner
K Studio Associato, Florence, Italy
T: +39 055 261961
E: michelegiordano@kpmg.it

Atty. Paola Casaccino
Attorney-at-law
Senior Manager
K Studio Associato, Florence, Italy
T: +39 055 261961
E: pcasaccino@kpmg.it

Atty. Alessandro Legnante
Attorney-at-law
Senior Legal Specialist
K Studio Associato, Florence, Italy
T: + 39 055 2619691
E: alegnante@kpmg.it

Latvia

A. **Cross border case results in so far highest fine in Latvia**

B. **“Apturi Covid” application – stop the virus with your phone!**

C. **Latvian Data Protection Authority’s opinion - service providers cannot demand a written confirmation about being abroad or health status**

Latvia

Cross border case results in so far highest fine in Latvia

The Latvian Data Protection Authority (LDPA) back in 2019 initiated an investigation which has resulted in so far highest fine amounting to 150 000 EUR against a controller for the failure to provide information to individuals on the use and collection of personal data and the failure to demonstrate compliance with personal data protection requirements – non-compliance with the principle of accountability.

The fine in question was applied by the LDPA following international cooperation initiated by the Spanish Data Protection Authority after a complaint from a Spanish citizen regarding misuse of its personal data by a Latvian registered e-commerce company.

The infringement of data subjects rights arose following the use of the online store of the Latvian company where the data subject placed an order and thereby transferred its personal data, namely, the name, surname, address and the mobile phone number to the company.

In the complaint submitted to the Spanish Data Protection Authority the person stated that prior to completing the order the opportunity to read the information of the contact details of the controller or the data protection officer, the purpose of the use of the personal data, the legal basis for the processing of the personal data, the period for which the personal data will be stored and other information required under the Article 13 of GDPR was deprived.

Following the investigation the LDPA concluded that while carrying out its commercial activity and thereby processing personal data of its customers the company has not ensured compliance with the principle of transparency and accountability secured under the GDPR. Having analysed the Privacy Policy of the company posted on the online store, the LDPA concluded that the information provided therein does not meet the requirements set under the GDPR.

Following its conclusions the LDPA imposed a fine in the amount of 150 000 EUR against the company for above mentioned data breaches. This LDPA decision was appealed in a court. The court made the final decision, maintaining the decision of LDPA in force.

Latvia

"Apturi Covid" application – stop the virus with your phone!

Many countries and companies nowadays have developed various tools with the purpose to limit the spread of COVID-19 and identify faster whether the person has been exposed to virus. Also Latvian leading IT companies in cooperation with medical professionals, epidemiologists and scientists have developed the application named – "Apturi Covid".

According to the information provided by epidemiologists, if this application would be by at least 20% of residents of Latvia, it will already be a great help for limiting the spread of COVID-19.

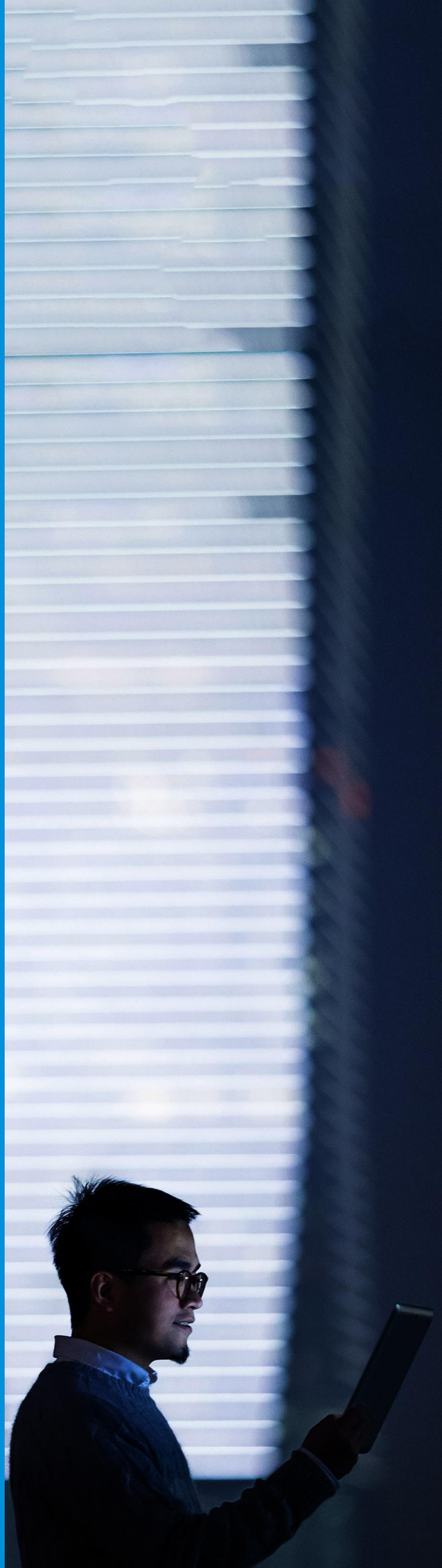
The functionality of "Apturi Covid" app is based on a methodology developed by scientists and the new Bluetooth signal exchange algorithm. The app uses Bluetooth function to anonymously detect nearby smartphones, which are within 2m proximity and present for longer than 15 minutes. The only condition for the successful use of this app is that the second person also must have this app installed on their smartphone. The information of the contact is only kept on user's device, and automatically deleted after 14 days, thereby no personal data is processed within the course of use of this app, except when the person has itself provided confirmation that in case of the confirmed contact with COVID-19 positive person it wishes to be contacted by the Latvian Centre of Disease Prevention and Control within the course of epidemiological investigation.

Latvia

"Apturi Covid" application – stop the virus with your phone! (cont.)

The use of this app is fully voluntary, but it is highly recommended. Everyone can start using it at any time and stop at any time as well. Also there are no fines or other sanctions for not using it in Latvia, but developers and experts note that everyone who have downloaded and uses this application play an essential part in helping Latvia and the whole world to limit the spread of COVID-19.

LDPA within its competence provided its support in the process of developing this app. There is no way for any user to get any data that could reveal who was the infected person. The application also itself does not identify a specific person and does not track a location of the person. LDPA emphasizes that it will monitor the observance of the individual's right to privacy, while providing an additional opportunity for the responsible authorities to protect the public health.



Latvia

Latvian Data Protection Authority's opinion - service providers cannot demand a written confirmation about being abroad or health status

Nowadays COVID-19 endangers the operation of all service providers – schools, shops, hospitals. Following the increase of COVID-19 positive cases these and also other service providers started to demand a written confirmation from the customers about the fact of being abroad or their health status. In its recent opinion the Latvian Data Protection Authority (LDPA) concluded that such processing of personal data has no legal basis.

Following the today's challenges a new tendency of the service providers (private companies, public authorities, organizations) wanting to protect their employees and customers from COVID-19 have been vastly observed. For this reason companies have started to develop their own methods: some survey the customer before the provision of the services, some require written confirmations or confirmations in the electronic form with the mandatory condition to provide name, surname, health status and information about being abroad.

Following review of this tendency against the GDPR the LDPA has brought an opinion and therewith explained that upon receipt of written confirmation, which contains above mentioned requested information, the service provider carries out processing personal data. In its opinion the LDPA has highlighted that the processing of personal data shall be based on at least on the one of the legal grounds indicated under the Article 6 of GDPR and should be proportionate to the aim pursued.

While the aim of such data processing could be limiting the spread of COVID-19 the health data of persons may only be obtained in accordance with the procedure which regulate processing of special category data. Having evaluated the GDPR and the local normative legal acts, the LDPA has concluded that the processing of such personal data (health related data) cannot achieve the possible processing aim - to limit the spread of Covid-19. Therefore, the LDPA has indicated that currently in Latvia there is no legal ground for carrying out such activities (obtaining confirmations) within the course of which health data is processed.

In its opinion the LDPA also provided recommendation for service providers that in order to limit the spread of Covid-19, instead of collecting person's confirmations, service providers can simply inform its customers about their responsibilities regarding the prevention of spread of COVID-19 laid down under the local regulatory acts.

Latvia

If you have any questions, please let us know

Una Petrauska
Law Firm Managing Partner, Attorney at Law
KPMG Law, Latvia
M: +371 67 038 031
E: upetrauska@kpmglaw.lv

Liene Mauriņa
Associate
KPMG Law, Latvia
M: +371 67 036 048
E: lmaurina@kpmglaw.lv

Poland

A. Penalties for lack of cooperation with the Polish Data Protection Authority

B. The employer has the right to require the employee to confirm legal residence in Poland

C. Keeping a register of stockholders

Penalties for lack of cooperation with the Polish Data Protection Authority

Lack of cooperation with the Polish Data Protection Authority (PDPA) by failing to reply to its letters or making it difficult for the PDPA to perform its tasks in any other way is a serious and quite frequent problem which PDPA faces during its work. In three such cases the PDPA decided to punish controllers.

The first fine in the amount of PLN 15 000 was imposed on the company involved in work placement in Poland and Germany for failing to provide the PDPA with access to personal data and other information necessary to carry out its tasks. A complaint against actions of this company was filed by a German citizen because it processed his personal data for marketing purposes. The complaint was lodged with the German Data Protection Authority competent for Rhineland-Palatinate, but it was taken over for consideration by the PDPA.

As part of the proceedings, the PDPA sent the company three times a call for explanations. Two of them (correctly delivered and received by the company) remained without any response. The company replied to one of the summonses, but the explanations contained therein were incomplete and contradictory

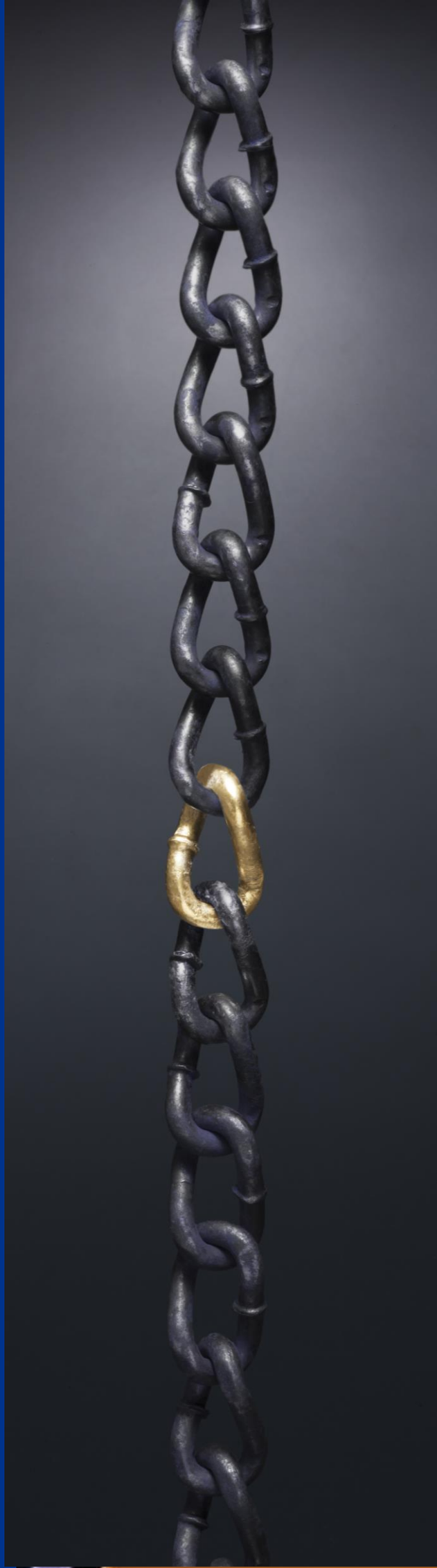
. In the opinion of the PDPA, they were far from sufficient to establish the facts of the case. In view of such company's conduct, the PDPA considered that the company deliberately impedes the course of proceedings or at least disregards its obligations related to cooperation with the supervisory authority. Therefore, the PDPA considered it necessary to initiate separate proceedings to impose an administrative fine on the company.

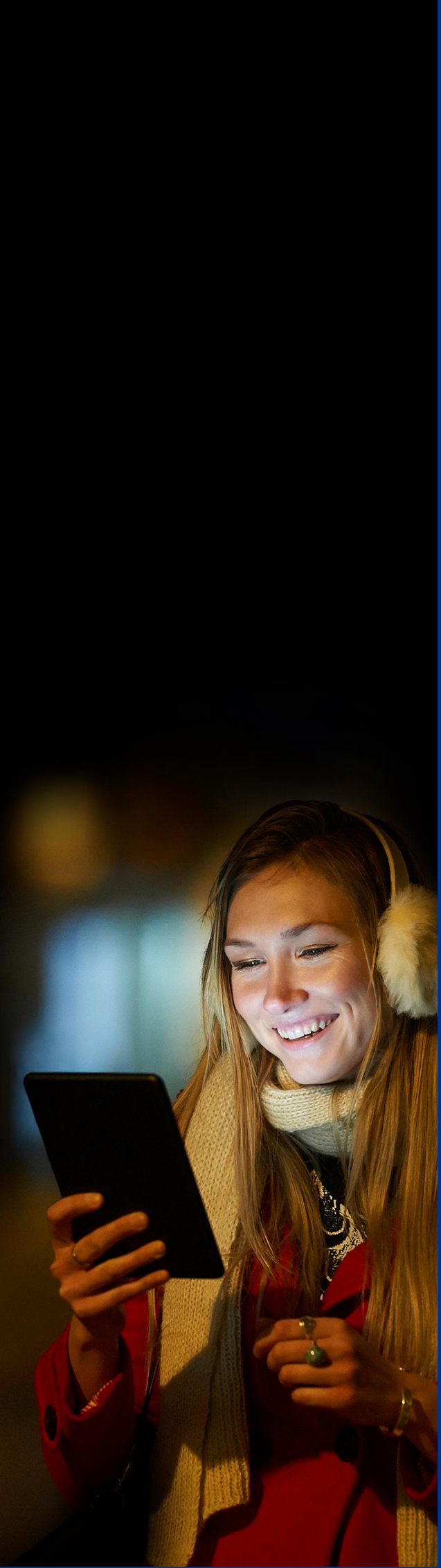
The second fine was imposed in the amount of PLN 5 000 on an individual entrepreneur running a non-public nursery and kindergarten. The entrepreneur reported to the PDPA violations consisting in loss of access to personal data stored. Due to the lack of information necessary to assess the breach, the supervisory authority sent the entrepreneur three times a request to provide relevant explanations. Two requests were not taken on time, while one of them the entrepreneur had received personally. The entrepreneur did not reply to the PDPA. The entrepreneur did not provide the PDPA with access to personal data and other information necessary for the performance of his tasks - in this case, to assess whether the controller, in a manner compliant with the provisions of the GDPR, notified the data subjects of the infringement.

Poland

Penalties for lack of cooperation with the Polish Data Protection Authority (cont.)

The third fine of PLN 100 000 (maximum amount for public entities) was imposed on the Chief Surveyor of the Country (*Główny Geodeta Kraju*). The PDPA has stated that the Chief Surveyor of the Country violated the provisions of the GDPR, consisting in the failure to provide the PDPA with access to the premises, equipment and means for processing personal data and access to personal data and information necessary for the PDPA for the performance of its tasks during the control. Moreover, the Chief did not cooperate with the PDPA during this control. Due to the Chief's categorical lack of consent to carry out control activities in their full scope and its unambiguously expressed lack of willingness to cooperate, the inspectors could not determine how and on what legal basis, when making land and building register information available through the GEOPORTAL2 (geoportal.gov.pl) internet portal, it enables access to personal data contained in land and mortgage registers and whether the Chief implemented appropriate technical measures to ensure data security. During the inspection it was not possible to examine what was the main subject of the inspection as it made it impossible to carry out all activities. In this respect, the inspection was thwarted by the Chief National Surveyor.





Poland

The employer is entitled to require the employee to confirm legal residence in Poland

The Polish Data Protection Authority recently issued a statement that an employer is entitled to demand the presentation of documents authorizing her or him to stay in the Republic of Poland.

According to the provisions of the Labor Code, the employer may process a closed catalogue of personal data of the applicant and the employee. These include the name and surname, date of birth, contact details, education, professional qualifications and the course of previous employment. However, the Labor Code gives the employer the possibility to request other personal data than those specified in this catalogue, if it is necessary to realize the right or fulfil the obligation resulting from the law. Such a situation will be dealt with by the controller in the case of employing a foreigner. The conditions for accepting persons who are not citizens of the Republic of Poland are specified by the provisions of separate acts.

The employer is obliged to do so by the Act of 15 June 2012 on the effects of entrusting the performance of work to foreigners staying in the territory of the Republic of Poland against the regulations. According to this Act, an entity entrusting the performance of work to a foreigner is obliged to demand from the foreigner to present a valid document authorizing her or him to stay in the territory of the Republic of Poland before starting work. What is more, the Act specifies that an employer who entrusts performance of work to a foreigner must keep a copy of this document throughout the whole period of performance of work by the foreigner.

Therefore, the processing of personal data concerning the stay in the territory of Poland, as it exceeds the catalogue indicated in the Labor Code, will take place on the basis of the legal obligation of the controller, i.e. the employer, in connection with the aforementioned provisions of the Act on the effects of entrusting work to foreigners staying in the territory of the Republic of Poland.

Poland

Keeping a register of stockholders

Entities legally entitled to keep the register of stockholders of companies that are not public companies, such as brokerage houses or custodian banks, are at the same time controllers of the data obtained for this purpose. They have their own, specified in the Commercial Companies Code, purposes for processing the data contained in the register.

An obligation to dematerialize shares is introduced in Poland. Companies based in Poland are obliged to choose and conclude a contract with the entity who dematerializes stocks and then keeps the register of stockholders of the company. In the opinion of the Polish Data Protection Authority, the companies and entities legally entitled to keep the register of company shareholders are separate controllers.

The register of stockholders is maintained by entities which are authorized to maintain securities accounts. Moreover, these entities are entitled to issue the registration certificates. This is their exclusive competence, not a task commissioned by the company, which also supports recognition of these entities as separate controllers. The entity keeping the register of stockholders, to which the company will provide the stockholders' data has its own purposes of processing the data contained in the register.

It would therefore be inappropriate practice for companies and entities maintaining a register of stockholders to enter into data processing agreements.

Poland

If you have any questions, please let us know

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

Romania

A. Statement of the Romanian Data Protection Authority on the obligations of entities developing or implementing location and tracking apps in the context of COVID-19 outbreak

B. Statement of the Romanian Data Protection Authority regarding the judgment of CJEU in Schrems II

C. Latest fines imposed by the Romanian Data Protection Authority

Romania

Statement of the Romanian Data Protection Authority on the obligations of entities developing or implementing location and tracking apps in the context of COVID-19 outbreak

The Romanian Data Protection Authority (RDPA) has announced that on the 21st of April 2020, the European Data Protection Board adopted Guidelines 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

The RDPA drew the attention on the necessity to comply with the rules of data protection, with the general principles relating to the processing of personal data, in particular the principles of privacy by design and privacy by default, the principle of ensuring the security and confidentiality, the principle of accountability, as well as on the necessity to respect the instructions set out by EDPB with regard to the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

The RDPA also emphasized that by EDPB's Guidelines 4/2020 it has been established for the tracking apps not to involve the use of location data, but only proximity data, as well as the fact that it is necessary for the controller to perform a data protection impact assessment (DPIA) prior to the implementation of this type of application, by taking into account the sensitive nature of personal data processed on a large scale.

Romania

Statement of the Romanian Data Protection Authority regarding the judgment of CJEU in Schrems II Case

The Romanian Data Protection Authority (RDPA) has informed that in Schrems II Case judgement, CJEU examined the validity of the European Commission Decision (EU) 2016/1250 in light of the requirements arising from the GDPR, taking into account the provisions of the Charter guaranteeing respect for the private and family life, personal data protection and the right to effective judicial protection

The RDPA emphasized that in the view of the CJEU, the Ombudsperson mechanism for the Privacy Shield does not provide guarantees equivalent to those required by the EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services.

Moreover, the RDPA accentuated that in the absence of an adequacy decision, the transfer of personal data to the US may take place in accordance with one of the following instruments provided by GDPR:

- standard data protection clauses;
- binding corporate rules;
- codes of conduct and certification mechanisms.

Also, the transfer of personal data to US may be performed under the derogations provided in GDPR.

Latest fines imposed by the Romanian Data Protection Authority

In the last three months (May-July) the Romanian Data Protection Authority (RDPA) has completed several investigations and applied seven fines amounting between 2,000 EUR and 15.000 EUR, as follows:

- Fine of 2,000 EUR applied to a postal services provider for failure to take the appropriate technical and organizational measures to prevent the unauthorized access to personal data (e-mail addresses and telephone numbers), which led to the compromise of the confidentiality of the personal data of 81 data subjects;

- Fine of 2,000 EUR applied to a non-banking financial institution for failure to handle the petitioner's request by which he exercises his right to erasure of data, and to provide the applicant with information on the actions taken following his request within a maximum of one month at his home address or contact address (e-mail), available in controller's records;

- Fine of 5,000 EUR applied to an airline company for non-compliance with the obligation to implement adequate technical and organizational measures in order to ensure that any natural person acting under the authority of the controller and who has access to personal data only processes them at the request of the controller, which led to the loss of confidentiality of personal data through the unauthorized access to data belonging to a number of five data subjects, as well as to the unauthorized disclosure of their data;

- Fine of 15,000 EUR applied to an automobile dealer for non-fulfillment of the obligation to implement adequate technical and organizational measures in order to ensure a level of security appropriate to the risk of processing for the rights and freedoms of individuals, which led to the unauthorized view and access to the personal data of a number of 436 customers of the controller and to the unauthorized disclosure of these data;

- Fine of 4,000 EUR applied to an energy company for non-fulfillment of the obligation to implement sufficient security and confidentiality measures to prevent the accidental disclosure of personal data to unauthorized persons, which led to sending documents containing data subject's personal data to another client of the controller using the electronic mail;

- Fine of 3,000 EUR applied to a telecommunications company for failure to implement sufficient security measures including verification of the accuracy of personal data collected by telephone for the purpose of concluding contracts, which led to an illegal processing of the data subject's personal data by concluding subscription contracts on data subject's name, using the personal data from a pre-existing contract, without verifying their correctness;

- Fine of 3,000 EUR applied to a cosmetics online store for processing personal data (name, surname, telephone number, date of birth and health information) without the consent of data subject or another legal ground.

If you have any questions, please let us know

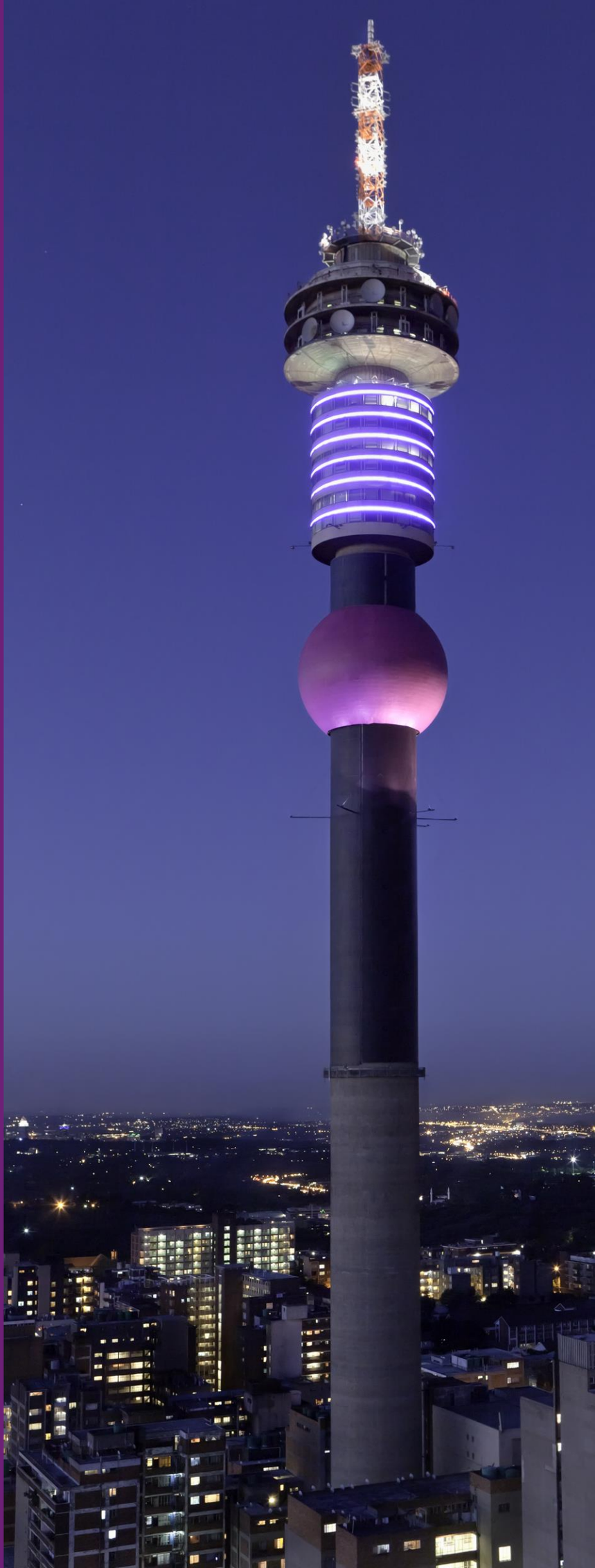
Cristiana Fernbach
Partner
KPMG Legal
T: +40 722 779 893
E: cfernbach@kpmg.com

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

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

South Africa

A. POPIA takes centre stage



POPIA takes centre stage

The South Africa government has recently breathed life into the Protection of Personal Information Act, 4 of 2013 ("POPIA").

Section 14 of the Constitution of the Republic of South Africa, 1996 (Constitution) provides everyone with the right to privacy. POPIA was enacted in order to give effect to section 14 of the Constitution, to promote the protection of information which is of a personal nature and which is processed by both public and private entities.

POPIA introduces conditions which need to be satisfied as minimum requirements in the context of the processing of personal information. POPIA is South Africa's equivalent of data protection laws found in many countries globally. POPIA provides an extensive list of what constitutes information of a personal nature (almost any information which relate to an identifiable, living natural person or an identifiable existing juristic person is considered personal information).

Although POPIA was promulgated in 2013, until recently only very limited sections were effective, namely the sections establishing the office of the Information Regulator, who is the regulatory authority in the context of matters related to personal information.

On 1 July 2020, the remaining substantive provisions of POPIA became effective, however, transitional arrangements are put in place which provide that entities have one year from 1 July 2020 to comply with POPIA.

Accordingly, all organizations have until 30 June 2021 to ensure that all processing of personal information complies with the requirements of POPIA. This includes compliance with the prescribed conditions for the lawful processing of personal information (which governs the receipt, collection, recording, use, modification, consultation, dissemination, storage, erasure and destruction of personal information, the security and confidentiality of personal information and the rights which data subject have with regards to their personal information).

POPIA not only applies to private and public entities in South Africa, but is also applicable to entities outside of South Africa that make use of automated or non-automated means for processing personal information in South Africa, unless such means are solely used to forward personal information through South Africa.

POPIA takes centre stage (cont.)

POPIA not only applies to private and public entities in South Africa, but is also applicable to entities outside of South Africa that make use of automated or non-automated means for processing personal information in South Africa, unless such means are solely used to forward personal information through South Africa.

Some of the key questions which need to be considered and addressed by South African organizations and those global companies with South African presence are:

— What type of personal information do we process and is there a lawful justification for continuing with that processing?

— Are we comfortable that the personal information is being stored securely?

— Do processes adequately cater for data subject rights and are we prepared to deal with data subject access requests?

— Do we transfer personal information to third parties for processing or do we transfer personal information outside of South Africa?

— Is your privacy governance structure fit for managing privacy risk and implementing your data strategy?

The penalties under POPIA may not be as harsh as some foreign jurisdictions (for example in Europe where some GDPR infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher).

However, the failure by private and public entities to comply with POPIA can have some severe consequences including imprisonment (for up to 10 years), the imposition of fines on such entities (up to ZAR 10 million) and/or civil claims for damages which may be brought by the person to whom the personal information relates.

POPIA compliance necessitates a thorough understanding of an organization's privacy risks and the existing controls in place to mitigate against those risks (whether internal or external to the organization). An assessment of how the organization processes personal information with reference to the requirements for the lawful processing of such personal information, as set out in POPIA, will be required as an initial first step in any POPIA compliance program.

Given the relatively short transitional period afforded by POPIA, organizations should already be well underway with their POPIA compliance programs. In this regard, we would expect organizations to have performed a POPIA gap analysis which identifies privacy risks within each business area and to be designing and implementing a privacy remediation plan.

South Africa

If you have any questions, please let us know

Nikki Pennel
Privacy Lead
KPMG Legal Services
T: +27 (0)82 719 5916
E: nikki.pennel@kpmg.co.za

Finn Elliot
Associate Director in Privacy team
KPMG Legal Services, South Africa
T: +27 (0)79 039 9367
E: finn.elliot@kpmg.co.za

Beulah Simpson
Manager in Privacy team
KPMG Legal Services, South Africa
T: +27 (0)60 602 3066
E: beulah.simpson@kpmg.co.za

Thato Mashishi
Consultant in Privacy team
KPMG Legal Services, South Africa
T: +27 (0)66 010 0167
E: thato.mashishi@kpmg.co.za

Spain

A. Radar COVID (Spanish government app for control of COVID pandemic) may be used

B. First sanction by the Spanish Data Protection Authority for failing to appoint a Data Protection Officer

C. The Spanish Data Protection Authority revisits its guidelines on the use of cookies to get them aligned with the new version of the EDPB's Guidelines 05/2020 on consent

D. The Spanish Data Protection Authority launches a tool to conduct speed /simple PIAs.

E. A new reality for Privacy as a result of COVID-19 crisis

Radar COVID (Spanish government app for control of COVID pandemic) may be used

Radar COVID has passed its testing phase satisfactorily and is now available to the health authorities of the autonomous communities, which will be able to connect this tool to their health notification management systems.

The Ministry of Economic Affairs and Digital Transformation ensures that the application complies with all the guarantees set by European regulations to safeguard the privacy of citizens.

The app developed uses a decentralized model, based on the Decentralized Privacy-Preserving Proximity Tracing protocol (DP-3T), and works as follows: the application uses Bluetooth connection, through which mobile phones emit and observe anonymous identifiers from other phones that change periodically. When two devices have been in proximity for 15 minutes or more at a distance of two meters or less, both save the anonymous identifier issued by the other.

If a user is diagnosed positive for COVID-19 after a PCR test, the user will decide whether to give consent for an anonymous notification to be sent through the health system.

Mobile phones that have been in contact with the patient would be warned about the risk of possible infection and instructions would be given on how to proceed. The Ministry states that, since no personal data are collected, it is impossible to identify or locate any user in any way.

On the other hand, the Ministry affirms that the Spanish Data Protection Authority (SDPA) has participated in the process prior to the implementation of the pilot experience; however, the SDPA has issued a statement affirming that its participation has been limited to initiating a procedure of prior investigation that has not yet concluded and that the lack of knowledge of the details of functioning of the application, essential for analyzing its impact on the privacy of citizens, has led to the requirement of formal requests for information to the Secretary of State for Digitalization and Artificial Intelligence and has prevented the assessment of its adequacy to the rules of personal data protection in advance.

Spain

First sanction by the Spanish Data Protection Authority for failing to appoint a Data Protection Officer

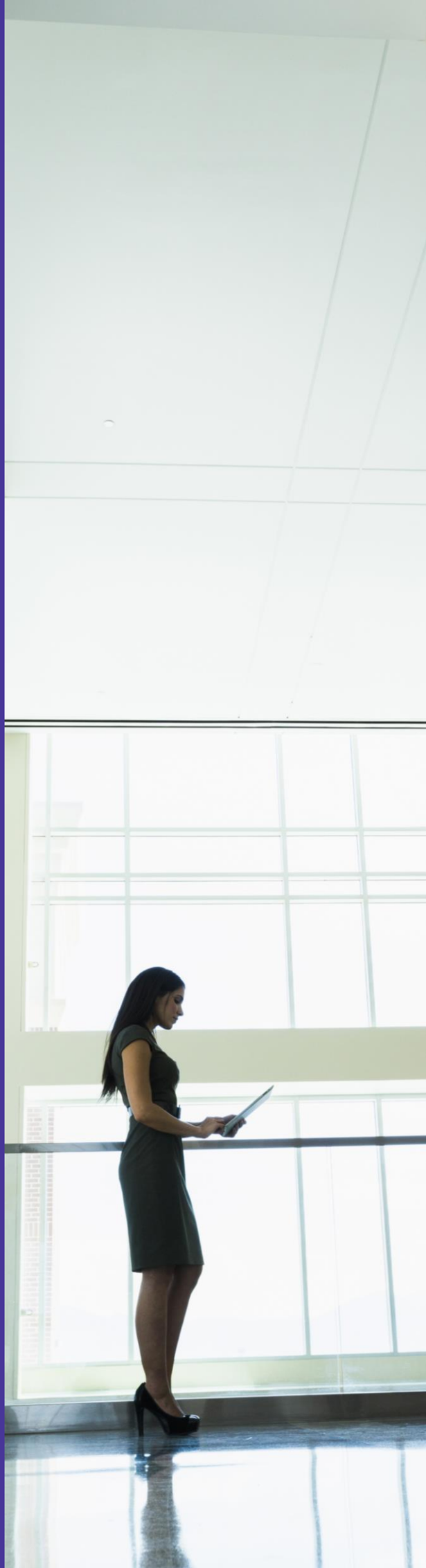
The Spanish Data Protection Authority (SDPA) sanctions a technology start-up company in the food delivery sector for not having appointed a Data Protection Officer (DPO).

The resolution was motivated by a complaint that two individuals filed before the SDPA in July 2019 for not having identified a DPO to which address data protection claims.

At the time of the complaint, the company had only appointed a data protection committee that carried out all the activities of a DPO. The company alleged that it was not included in any of the cases established in the RGPD or in the Spanish Data Protection Act that require such designation and therefore, it is exempt from the obligation to designate a DPO.

However, the SDPA considered that the constitution of a data protection committee is not sufficient to comply with the provisions of such regulations, especially since there was not even a mention of it on its public privacy policy and none of its members was registered as a DPO in the Register of Data Protection Officers of the SDPA.

Consequently, the SDPA considers that due to the type of activity carried out by the company, which carries out large-scale processing of personal data, the lack of designation of DPO leads to the infringement of the applicable data protection regulations, which carried a penalty, in that case, of EUR 25,000.



Spain

The Spanish Data Protection Authority revisits its guidelines on the use of cookies to get them aligned with the new version of the EDPB 's Guidelines 05/2020 on consent

The new version of the Guide adapts its content to the Consent Guidelines reviewed by the European Data Protection Board in May of this year

The European Data Protection Board (EDPB) in May 2020 reviewed the Guidelines 05/2020 on consent in order to clarify its position in relation to two issues: the validity of the option "continue browsing" as a way of providing consent by users and the possibility of using the so-called "cookie walls", i.e. limiting access to certain services or content only to users who accept the use of cookies.

Consequently, the Spanish Data Protection Authority has updated its guide on cookies to adapt it to the criteria established by the EDPB in relation to these two issues, clarifying that:

- The option "continue browsing" does not, under any circumstances, constitute a valid way of giving consent, insofar as such actions may be difficult to distinguish from other user activities or interactions, so that it would not be possible to understand that consent is unequivocal.

- In order for a cookie wall to be used, access to the service and its functionalities must not be conditioned on the user's consent to the use of cookies, so an alternative to consent must be offered.

The new criteria must be implemented no later than 31 October 2020, thus establishing a transitional period of three months for those websites which consent is not being obtained in accordance with the new guidelines requirements, to introduce the necessary changes in the mechanisms to obtain consent for the use of cookies.

Spain

The Spanish Data Protection Authority launches a tool to conduct speed /simple PIAs.

This tool helps companies and administrations performing high-risk data processing activities to carry out risk analysis and impact assessments

The free tool Gestiona_EIPD guides data controllers and processors in all the aspects that must be taken into account in performing risk analysis and impact assessments, providing an initial basis for carrying out an appropriate risk management, including the applicable regulatory compliance requirements and possible measures aimed at reducing or mitigating risks.

This tool is designed as an online questionnaire where the controller or processor must assess in first placer whether he wants to make a risk analysis or an impact assessment on data protection.

The data provided by the controllers and processors within this tool will allow them to obtain this basic documentation. The process must be completed following the indications established in the Practical Guide for Conducting Data Protection Impact Assessments subject to the RGPD, and periodically analyzed so that at all times it can be demonstrated that the processing is carried out in accordance with the requirements established in the data protection regulations.

A new reality for Privacy as a result of COVID-19 crisis

KPMG's Spanish team analyses the privacy risks arisen from the use of new technologies in the fight against COVID-19 crisis, based on the study published by the Spanish Data Protection Authority (SDPA) last May 2020.

As a consequence of the health crisis caused by COVID-19, the use of technology is becoming a key factor in adapting the performance of normal activities to the new way of life. This digital transformation provides several advantages to the society, supporting the development of such activities in a safety manner and minimizing the risk of infection by coronavirus.

In this context, it becomes crucial to determine if these activities, which mostly involve the processing of personal data, are carried out in a proportional manner, establishing an appropriate balance between the advantages obtained and the impact caused to the data subjects.

KPMG's Spanish team, based on the study published by the SDPA "The use of technologies in the fight against COVID-19", has performed a high-level analysis of the main privacy and data protection risks and implications emerging from the use of disruptive technologies in COVID-19 crisis.

. As an example, temperature reading systems and contact-tracing applications were included as part of this analysis:

Regarding the temperature reading systems, the main risks identified correspond to the lack of accuracy in the data collected, not guaranteeing that measurements are based on reliable and precise intervals, the unauthorized disclosure of health data, if measurements are taken in public, and the absence of legitime basis for the processing, if any establishment does so without the appropriate analysis and justification.

Contact-tracing applications main risks involve the lack of explicit and legitimate processing purposes, if the app is used for additional purposes such as study behavioral patterns or large-scale video surveillance, and the lack of robustness in the anonymization protocols, allowing the re-identification of individuals in the network.

Technological advances and the ability to innovate and improve our lives are great news. However, we must never forget the respect for the maximum protection of the data involved in these activities by adopting a risk-based approach from the early stages of the projects. This approach should consider aspects such as the performance of a Data protection Impact Assessment, the application of Privacy by Design process and the implementation of appropriate technical and organizational measures, among others.

If you have any questions, please let us know

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

Lorena Jurado
Manager
KPMG in Spain
T: +34 (0) 620 190 335
E: ljurado@kpmg.es

Eric Romero
Manager
KPMG in Spain
T: +34 93 2532903
E: ericromero@kpmg.es

Ana de la Higuera
Senior Associate
KPMG in Spain
T: +34 (0) 679 676 138
E: adelahiguera@kpmg.es

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

Maria Benito
Senior Associate
KPMG in Spain
T: +34 (0) 616 949 502
E: mariabenito@kpmg.es

Turkey

Public Announcements from Turkish Data Protection Authority

The Turkish Data Protection Authority (TDPA) published various public announcements regarding the protection of personal data

Public Announcement Regarding the Deadline for Registration

TDPA announced that the deadline for registration to VERBİS (Data Controllers Registry System) has postponed once again.

According to the announcement;

- data controllers residing/registered abroad and data controllers with more than 50 employees annually or an annual financial balance of more than 25 million Turkish Liras shall register until 30.09.2020,
- data controllers with less than 50 employees annually or an annual financial balance of less than 25 million Turkish Liras but whose main business activity is processing special categories of personal data shall register until 31.03.2021 and
- data controllers that are public institutions and organizations shall register until 31.03.2021.

Public announcement on requests to delist

TDPA announced the criteria to be considered when assessing requests to delist the results displayed following a search based on person's name and surname from a search engine's index.

The TDPA determined that right to request that the results related to the person not be achieved in searches made by the name and surname of the search engines is defined as a request to be removed from the index.

Considering that search engines determine the purposes and means of processing the data collected by third parties on the internet, they are accepted as data controller and the data subjects should first apply to the search engines regarding their requests to remove the search results from the index, if the data controller search engines refuse such requests or do not respond to the applicant, data subjects can complain to the TDPA.

It is also possible for data subjects to apply directly to the legal authorities while applying to the TDPA if their requests are rejected by the data controller search engines or if their requests are not answered.

Data breaches

Data breach notifications published by the Turkish Data Protection Authority (TDPA)

The TDPA has published several data breach notifications on its official website since the previous newsletter. These notifications include data controllers such as insurance and pension companies, banks and various retail companies. One of the most significant and recent notification published on the official website is related to a data breach that occurred in a well-known job-search website (Company);

- The breach was detected by a consultant serving as a supplier to the Company on August 12, 2020, by informing an employee of the Company that a file allegedly belonging to 50,000 members of the said website was uploaded to another website on the same day,
- The violation occurred on August 10, 2020, and it was detected by the Company on August 12, 2020,
- The data affected by the breach are "email address", "user password", "name and surname", "date of birth", "phone number", "profile photo", "URL link information", "city of residence", "district of residence",
- The number of people affected by the violation is 40.955 and the number of records is 53.149.

If you have any questions, please let us know

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

UK

A. Data transfers to the US and to the UK post Brexit in question after CJEU's Schrems II Judgment

B. Information Commissioner Office (ICO) releases FAQs on data protection following the end of the Brexit transition period

C. Court of Appeal hands down judgement in R (Bridges) v Chief Constable of South Wales Police regarding the use of Facial Recognition by the police

D. The ICO launches new guidance on AI and data protection

United Kingdom

Data transfers to the US and to the UK post Brexit in question after CJEU's Schrems II Judgment

On 16 July 2020 the Schrems II Judgment from the EU Court of Justice (C-311/18) was published. This is the latest chapter in the Schrems case that took down the former EU-US Safe Harbour scheme in 2015. There are two important takeaways provided by the judgment that will trigger changes to numerous companies' cross-border data transfers arrangements:

- First, the US Privacy Shield is no longer valid. The "Privacy Shield" data sharing mechanism between the EU and the US is invalid. The CJEU has declared that the remedies prescribed under Privacy Shield are not sufficient to protect personal data from US surveillance and security laws. Organizations can no longer transfer personal data to the US based on a Privacy Shield certification.

- Secondly, Standard Contractual Clauses remain in force with additional obligations. Putting in place European Standard Contractual Clauses for the transfer of personal data to countries outside the EU and without an adequacy decision remain valid, however organizations will be responsible for determining whether the protections in the country without an adequacy decision meet EU standards in the context of the specific transfer.

Since the judgment sets out that US surveillance and security laws are the reason the Privacy Shield decision was declared invalid, at this stage the biggest question is around how international transfers to the US based on Standard Contractual Clauses and intra-group transfers to the US relying on Binding Corporate Rules may be compliant with GDPR except based on consent or an Article 49 derogation.

The European Data Protection Board published a FAQs document in this regard on 24 July stating that Standard Contractual Clauses and Binding Corporate Rules may be used for international data transfers to the US with supplemental measures, but it was not described what these are, so further directions on this are expected to come. Besides, the Information Commissioner Office (United Kingdom's Data Protection Authority) announced that controllers in the UK could continue to rely on their current arrangements until further guidance is developed.

This judgment will have a significant impact on data flows from the EU to the US, and potentially to other third countries with strict security laws and wide surveillance laws and has also highlighted that post-Brexit, when the UK becomes a country without an adequate level of protection, the UK can expect its surveillance regime and the UK-US October 2019 agreement to come under close scrutiny as it seeks an adequacy decision.

United Kingdom

Information Commissioner Office (ICO) releases FAQs on data protection following the end of the Brexit transition period

These FAQs offer further details on how the ICO envisages the data protection landscape after 31st December 2020, including information a range of topics such as:

- Whether businesses will need a European representative;
- Transferring data to and from Europe in the event of a no-deal; and
- The UK government's approach to EU commission adequacy decisions,

along with links to further guidance on most questions. The FAQs also confirm that EU laws such as the PECR, NIS, and EIR will continue to apply, either by virtue of already being set out in UK law or because the government intends to incorporate them into UK law following 31st December.

United Kingdom

Court of Appeal hands down judgement in R (Bridges) v Chief Constable of South Wales Police regarding the use of Facial Recognition by the police

In a brief online statement, the ICO welcomed the outcome of the appeal in this landmark case on the use of live Automated Facial recognition technology ("AFR") by the police which achieved mixed success for the Appellant. The judges were unanimous on the following:

1. that the divisional court had erred in considering South Wales Police's ("SWP") interference with the Appellant's right to privacy to be in accordance with the law;

2. in principle, SWP's use of AFR was a proportionate interference with the Appellant's Art.8 rights (NB - the court merely addressed this ground of appeal for completeness, since 1 (above) negates the need to consider proportionality);

3. the DPIA conducted by SWP was deficient;

4. SWP had no need of an appropriate policy document (as per s.42 DPA 2018), as its deployment of AFR predated the DPA 2018's coming into force; and

5. that SWP failed to take reasonable steps to ensure their AFR software had no inherent racial or sexual bias (although the court noted there was no clear evidence in this case that it did exhibit any such bias).

According to the Press Summary, SWP has no intention of appealing against the judgement, in spite of the Appellant's success on the main aspects of the case.

United Kingdom

The ICO launches new guidance on AI and data protection

The ICO has published new guidance on AI and data protection. It covers best practices for data protection-compliant AI solutions, interpretation on how data protection law applies to AI systems that process personal data and recommendations on organizational and technical measures to mitigate the risks to individuals that AI may cause or exacerbate.

This guidance is aimed at two audiences:

- those with a compliance focus, such as data protection officers (DPOs), general counsel, risk managers, senior management, and the ICO's own auditors; and
- technology specialists, including machine learning experts, data scientists, software developers and engineers, and cybersecurity and IT risk managers.

The guidance clarifies how organizations can assess the risks to rights and freedoms that AI can pose from a data protection perspective; and the appropriate measures that can implemented to mitigate them.

United Kingdom

If you have any questions, please let us know

Isabel Ost
Director
Solicitor
KPMG Law in the UK
T: +44 (0)7818 588 789
E: Isabel.Ost@kpmg.co.uk