KPMG

Data privacy newsletter

KPMG Global Legal Services

January - February 2020

Contents

Introduction

Welcome to the fourth edition of KPMG Global Legal Services newsletter, covering developments in the world of data protection and privacy law.
KPMG member firms are rightly proud of the global network, KPMG privacy lawyers and professionals are committed to offering clients the highest quality services in this area.

In this publication we bring you snapshots of recent developments in a selection of the jurisdictions. We live in fast changing times, and 2019 was a busy year for GDPR. Under new data protection rules, the rights of every individual living in the EU are now better protected and public awareness about the value of online privacy is at an all-time high. Our publication seeks to share the development of legislation in various jurisdictions, whilst also showing the very broad impact that data protection law can have.

International

SCHREMS II and Opinion of Advocate General (AG) of December 2019

Anticipating the decision on the second court case of Maximliam Schrems with the CJEU regarding International data transfers to USA, standard contractual clauses (SCC) and the Privacy Shield, the Advocate General (AG) issued his Opinion, which provides that:

a) SCCs are valid, as they provide a general mechanism applicable to transfers of personal data to third countries and the appropriate safeguards guarantee the appropriate level of protection,

b) the SCCs' main purpose is to compensate for any deficiencies in the protection afforded by the third country of destination, which the parties contractually undertake to respect,

c) the question of whether the compensation is adequate does not relate with the level of protection guaranteed in the third country,

d) the compatibility of SCCs with the EU Charter of Fundamental Rights depends on whether there are adequate mechanisms to ensure that when the SCCs are breached or impossible to honor, the transfers based on SCCs are suspended or prohibited,

e) the AG reiterated that the subject matter of the proceeding relates to the validity of the SCCs and the validity of the Privacy Shield will not influence the outcome of the proceeding and that the organizations should be able to ensure that SCCs are being complied with, otherwise a supervisory authority should suspend the transfer.

International

The European Data Protection Board (EDPB) adopted draft Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

As vehicles become increasingly more connected, the amount of data generated about drivers and passengers by these connected vehicles is growing rapidly. The EDPB guidelines focus on the processing of personal data in relation to the non-professional use of connected vehicles by data subjects. More specifically, the guidelines deal with the personal data processed by the vehicle and the data communicated by the vehicle as a connected device. The guidelines will be submitted for public consultation.

The Draft Guidelines are released for public consultation until March 20th at the latest.

Belgium

- First Cookie fine imposed by Belgian DPA
- First post GDPR recommendation of the Belgian DPA

First Cookie fine imposed by Belgian DPA

On 17 December 2019, the Belgian Data Protection Authority ("DPA") imposed an administrative fine of EUR 15 000 on a company that manages a website with legal news and information. It is the first decision that is published by the Belgian DPA regarding an online platform.

Findings of Belgian DPA's inspection service

Cookie requirements

Initially, the company's website made use of cookies without asking for a valid consent and subsequently using a cookie banner with pre-ticked boxes to obtain consent.

This practice was already found unlawful by the European Court of Justice in the past as it does not qualify as an 'active consent' (i.e. active action such as ticking the box) and has been confirmed by the Belgian DPA in its judgement. Furthermore, there was no possibility for the data subject to withdraw his/her consent easily.

Information requirement

The information to be provided to the visitors of the website was found to be incomplete. Among other things, the data controller's identity and contact information as well as the data subjects' rights and the retention period for personal data collected by the cookies were not specified.

Transparency

The information concerning the processing of personal data was found not to be adequately transparent. In practice, the company's website is directed at Dutch and French-speaking data subjects. However, the company's privacy policy was initially only available in English making reference to privacy legislation of the USA.

With its administrative fine of EUR 15 000 the DPA has taken a clear position that all website providers in Belgium have to respect the applicable privacy (and cookie) legislation.

First post GDPR recommendation of the Belgian DPA

On 17 January 2020 the Belgian DPA has published new guidelines relating to the processing of personal data for direct marketing purposes. By introducing these new guidelines the Belgian DPA wanted to create more (legal) certainty for companies and organizations on how to be compliant with the GDPR when making use of "direct marketing".

What is "Direct Marketing"?

In its guidelines the Belgian DPA provided for a definition of what is to be understood under direct marketing:

Any communication, in any form, solicited or unsolicited, originating from an organisation or a natural person and directed at the promotion or sales of services, goods (whether or not against payment) as well as trademarks or ideas, addressed by an organisation or natural person active in a commercial or non-commercial context, which is directly directed to one or more natural persons in a private or professional context and which entails the processing of personal data.

Furthermore, the Belgian DPA has clarified every element of this definition by making use of practical examples.

How to be compliant and protect the personal data when making use of direct marketing?

The Belgian DPA has made several recommendations in its guidelines on how to be compliant and protect personal data. Moreover it has identified several elements that need to be taken into account when processing personal data for direct marketing purposes:

- Qualify all actors and GDPR provisions that are involved in the direct marketing process;
- Determine the processing purposes;
- Define the processing operations;
- Identify the data that is required for your purpose;
- Verify your legal processing ground when processing personal data for direct marketing purposes;
- Be transparent with the data subject.

The Belgian DPA further explains the lawful and appropriate legal basis (including criteria that need to be complied with) for the processing of the personal data for direct marketing purposes and has indicated that more guidelines will be published in the near future.

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

- **The Commission for Personal Data Protection bans placing video cameras on street posts**
- **The Commission for Personal Data Protection ruled in favour of website operator in a data subject rights dispute**

The Commission for Personal Data Protection bans placing video cameras on street posts

The CPDP issued a formal instruction to a controller to cease any video surveillance over publicly accessible areas – roads and pedestrian areas, as well as over residential buildings and other property not owned by the controller.

The Commission for Personal Data Protection (CPDP) was presented with a complaint from an individual stating that a neighboring car repair service's proprietor conducts video surveillance over a publicly accessible areas as well as over the claimant's home. The cameras in question was placed on street posts and covered the roads and pedestrian areas.

A police report was presented before the CPDP evidencing that the claimant's home was not under surveillance, the CPDP stated that police authorities are not entitled to deal with data protection matter and presided over the case.

In the course of the proceedings, the CPDP actually established that the claimant's home is not under surveillance directly. Despite that, the CPDP analyzed the lawfulness and fairness of the car service's video surveillance system.

The CPDP ruled that data processing via video cameras is lawful and admissible only as far as it concern the car service proprietor's premises. Therefore, cameras placed there and covering that area may remain in use. The CPDP explained that this processing falls within the legitimate interests of the controller to safeguard his property. As for all cameras that were placed on public infrastructure and covered publicly accessible areas and other peoples' homes, the CPDP rendered that processing unlawful.

The CPDP issued a formal instruction to the controller to cease any video surveillance over publicly accessible areas – roads and pedestrian areas, as well as over residential buildings and other property not owned by the controller.

The Commission for Personal Data Protection ruled in favour of website operator in a data subject rights dispute

The Commission for Personal Data Protection denied complaint from a website's customer bringing false claims against the data controller

A website customer argued before the Commission for Personal Data Protection (CPDP) that a subject request was filed for all the customer's personal data and all his profiles in the controller's database to be deleted. Furthermore, the customer stated that he thereby withdrew his consent for processing his personal data in any manner, for whatever purposes.

The website operator contested the claims of the customer and argued that all that was requested by the customer was actually granted. The website operator produced copies of correspondence before the CPDP to support its claims.

It was established that the customer had two separate profiles registered, which was in violation of the website's general terms of use. When the customer reached the website operator, the controller informed the customer that one of the profiles must be erased and provided him with the option to choose which one to remain active.

During the proceedings before the CPDP, the website operator provided its formal reply evidencing that Profile No. 1 was deleted, and Profile No. 2 remained active in compliance with the customer's request. Moreover, the website operator provided instructions to the customer on how to delete the remaining profile, as well.

The CPDP ruled that the controller fulfilled all its obligations to provide assistance to the data subject and to comply with the data subject's requests and repealed the customer's claim.

If you have any questions, please let us know

Juliana Mateeva

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

Siana Garbolino

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

Teodor Mihalev

Lawyer, Legal Advisory
KPMG Bulgaria
T: +35929697600
E: tmihalev@kpmg.com

Czech Republic

- Overview of inspections for the second half of 2019
- Investigation of a major software company with respect to selling customers' personal data
- The Office reported about the matter of sending business communications
- The Office updated its opinion on data protection impact assessments (DPIA)

Overview of inspections for the second half of 2019

Recently published overview of the Czech Data Protection Office (hereinafter only the "Office") contains information on completed inspections for the second half of the previous year. The inspections covered a diverse range of matters.

The Office imposed the highest fines for unsolicited commercial communications regarding financial services, the sale of commemorative medals, mobile tariffs and various other products and services. These inspections were most often initiated following complaints raised by the data subjects. Other inspections can be divided into several categories, in particular – financial services, IT, public administration, sale of goods and services, employment, telecommunication, healthcare, social services and others.

The Office in connection with the commercial communications, highlighted that the ease of accessibility of some personal data a priori does not create the possibility of their unlimited processing. The controller must always have a legal ground to process personal data under Article 6 of GDPR, even for published personal data.

Investigation of a major software company with respect to selling customers' personal data

At the end of January 2020, a Czech software company was publicly accused of controversial monetization of its customers' personal data. The whole case commenced when two international online servers released their investigations claiming severe allegations regarding the personal data operations of this company and its subsidiary.

The allegations concerned the fact that the company was gathering its customers' personal data and subsequently sold them to third parties. The main issue was that although the data were in an anonymized form, it was possible to identify specific data subjects. The data subjects thus remained identifiable.

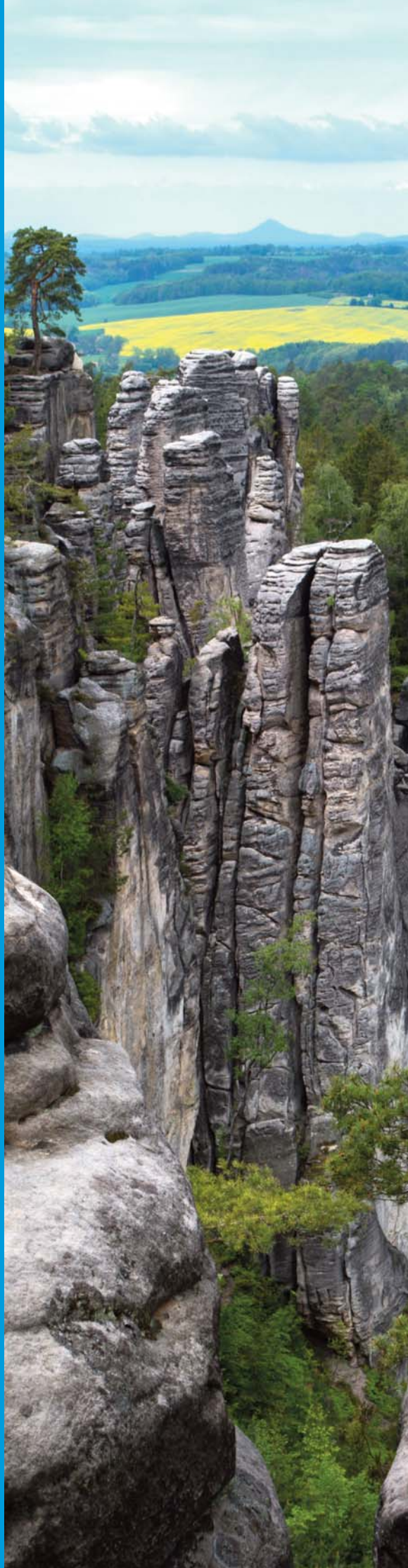
In response to such allegations, the company in question released an apology and terminated the business operations of its subsidiary which actually carried out the selling of the data. The Office issued an official statement stating that they are gathering necessary information and that there is a suspicion of a serious breach of data subjects' privacy.

The Office reported about the matter of sending business communications

The Office reported that they receive a large number of complaints about the sending of unsolicited commercial communications.

The Office's supervisory practice revealed many cases in which commercial communications were sent by third parties other than entities to which the data subjects provided their consent. These senders were often companies with foreign domain addresses who were carrying out the communication based on an authorization from the respective entrepreneur/business/company. The Office warned that in such case the ordering party often loses control over who is actually delivering the communications, and in particular whether the commercial communications are sent only to the contact details (e-mail address, telephone number) of the addressees who have given proper consent to receive the commercial communication.

The Office stressed that the data controllers who order or initiate such mailing activities (for example by using affiliate services or lead marketing tools) are still required to be able to prove that they have the consent of the recipients of the commercial communication or to secure such consent through the mailing company.



The Office updated its opinion on data protection impact assessments (DPIA)

The document now provides conclusions both on processing operations that are and that are not subject to the impact assessment. It is now published under the heading "List of types of processing operations (not) subject to the data protection impact assessment requirement".

The material is intended to help the data controllers to decide whether or not a particular processing is subject to the DPIA obligation. The document was compiled taking into consideration the Office's previous supervisory practice, its list of processing operations which are subject to the DPIA established under Article 35 (4) of GDPR, and the negative list established under Article 35 (5) of GDPR. The negative list of operations that are not subject to the DPIA should aim to not burden small and medium-sized controllers performing common non-risk processing. The document is available here.

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

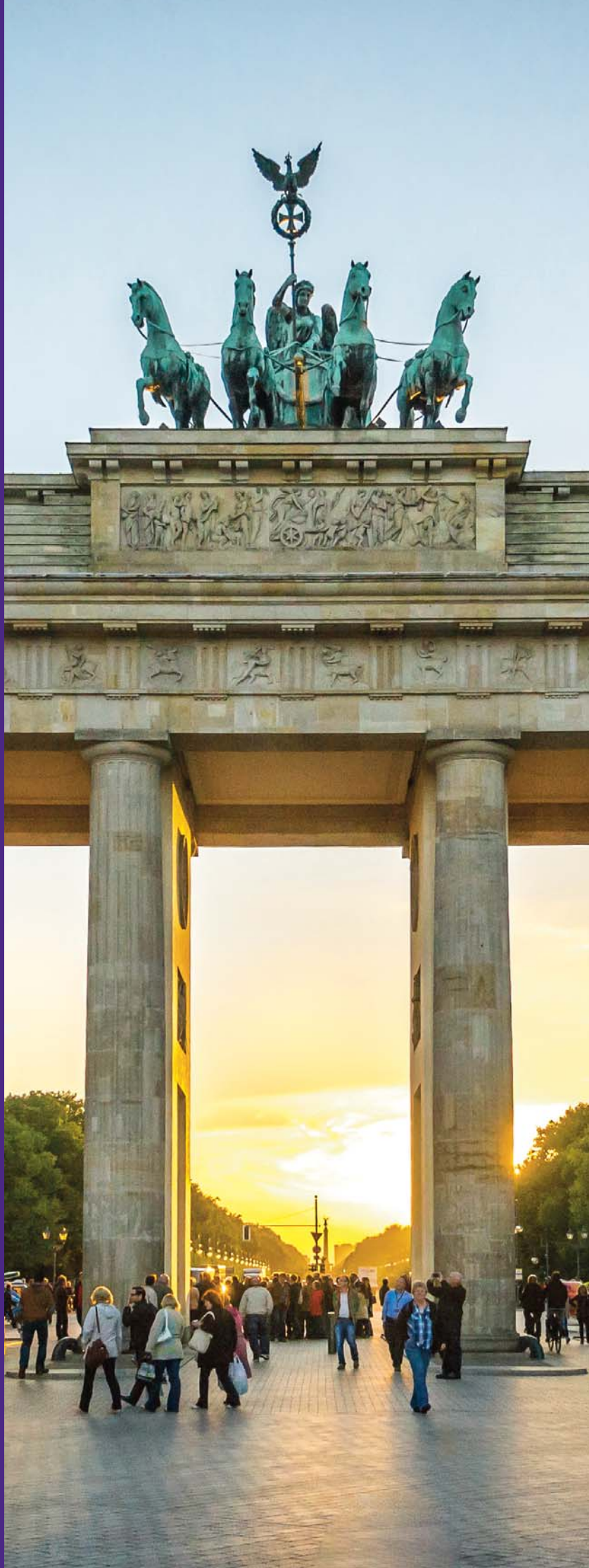
Associate Manager
KPMG in the Czech Republic
T: +420 222 123 169
E: fhorak@kpmg.cz

Ladislav Karas

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

Germany

- **Data Protection Officer of Baden-Wurttemberg issues guidelines on the use of social media for public bodies**
- **The Federal Commissioner for Data Protection and Freedom of Information (BfDI) launches consultation process on anonymization of data**
- **Draft of the Patient Data Protection Act in the Telematics Infrastructure**



Data Protection Officer of Baden-Wurttemberg issues guidelines on the use of social media for public bodies

The Data Protection Officer of Baden-Wurttemberg has shut down his account on Twitter. The account had attracted numerous followers as it regularly contained interesting and crucial insight in the work if the authority. Numerous opinions on legal questions had (first) been published on this channel. The shutdown has not gone unnoticed and has been used by the Data Protection Officer of Baden-Wurttemberg to publicly criticize the (in his eyes) unreflected use of social media networks by public bodies as well as companies.

In the eyes of the Data Protection Officer of Baden-Wurttemberg, the use of social media networks is extremely critical in light of the recent decisions by the European Court of Justice. According to these decisions, there will usually be a joint control (Art. 26 GDPR) between the social media network and the operator of the "site" or "channel" with regard to the collection of personal data on the social media network. However (so the statement), the social media networks were rather vague in the description which data is collected. Additionally, the joint control agreements provided (if any) by the social media networks would not meet the necessary legal threshold. Therefore, the use of social media networks could only be regarded as unlawful at this moment.

The guidelines published by the authority list numerous prerequisites for the use of social media networks by public bodies. The most important prerequisites are as follows:

- There has to be a legal justification for the collection of personal data, to be assessed by the public body.
- The transparency rules from the GDPR have to be adhered to.
- There has to be a sufficient agreement on the joint control.
- The public body has to provide alternative means of communication for citizens.
- The necessary technical and organisational measures have to be implemented.

The Data Protection Officer of Baden-Wurttemberg notes that his authority is well aware that it will be impossible to follow these guidelines without cooperation of the social media networks. However, it is also stated very frankly that a lack of cooperation can only be answered by leaving the social media network.

The authorities are apparently of the impression that the social media networks still lack sufficient data protection. Although the GDPR meant to harmonize the data protection rules across the EU, the authorities in Germany feel that there is not enough pressure on the social media networks.

They have now chosen once again an approach where the authorities – publicly confirmed by numerous authorities – put the pressure on public bodies and companies. The apparent hope is that once there is enough pressure from public bodies and companies, the networks will be forced to change their own approach on data protection.

The Data Protection Officer of Baden-Wurttemberg states that "the grace period" would be over now. They would now first go after public bodies and the companies. It remains to be seen whether this will amount to (significant) fines.

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) launches consultation process on anonymization of data

On February 20th, the BfDi has launched a public consultation procedure to obtain comments and opinions on "anonymization under the GDPR". The consultation is being carried out with particular attention to the telecommunications sector, but the basic question concerns all companies involved in the anonymization of data.

The aim of the consultation is to clarify the current legal framework for anonymization of personal data by persons responsible from the point of view of the BfDi and to initiate public discussion about it. The BfDi clearly states that per his opinion anonymization is data processing that needs a legal basis to be in accordance with data protection law. The argument of the BfDi is rather simple and relates to the fact that anonymization requires that the personal reference of the data be removed. To do this, the data must be changed by removing individual elements of it.

Regarding the legal basis the consultation paper mentions various possible articles of the GDPR as well as of the German Telecommunications Act (TKG). The BfDI is of the view that it must be decided case-by-case which legal justification for the process of anonymization is applicable.

The background of the consulation is rather releveant for practice. Anonymization of data can, on the one hand, realize the "principle of data minimisation" according to Art. 5(1)(c) GDPR. On the other hand, anonymization can also enable data to be processed in the first place, because in some areas data relating to individuals would otherwise not be allowed to be processed at all (the particularly sensitive area of health data should be considered in particular). Some companies are therefore dependent on working with data that has already been anonymized or on being able to anonymize data that they have in their possession with personal reference.

Anonymous and anonymised data are mentioned in sentences 4 and 5 of recital 26. According to this, the principles of data protection does not apply to anonymous information, "i.e. information that does not relate to an identified or identifiable natural person, or personal data that have been made anonymous in such a way that the data subject cannot or can no longer be identified". The GDPR does not contain any further provisions in this respect. It is therefore generally disputed if anonymization is "data processing" in the sense of the GDPR and needs a legal justification. It is strongly debated on which legal basis the anonymization may be based.

However, the BfDI makes it clear that from his point of view anonymization is data processing and needs a legal justification. Nevertheless, the BfDi stresses the case-by-case approach to be taken when evaluating the legal justification. The BfDi however also points out that the obligation to erase data can be fulfilled by anonymizing.

Until March 9th, 2020 interested stakeholders, which are concerned with this topic can now submit their comments and statements to the BfDi.

The BfDi plans to release a position statement once interested stakeholders have submitted their comments and statements.

Draft of the Patient Data Protection Act in the Telematics Infrastructure

According to the new Digital Supply Act ("DVG"), health-insured persons must be offered an electronic patient file ("ePA") by health insurance companies from 2021 onwards. To specify the requirements under data protection law resulting from the DVG and to make the possibilities and advantages of electronic patient files available to all insured persons, the German Federal Ministry of Health has drafted the Patient Data Protection Act in the Telematics Infrastructure ("PDSG"), which provides considerable adjustments to Volume 5 of the Social Insurance Code ("SGB V"), in particular to the section on telematics infrastructure.

The digitization of health data is intended to improve health care, but also to facilitate communication between the parties concerned. Therefore, the PDSG shall bring digital solutions quickly to the patient and protect sensitive health data in the best possible way.

The PDSG grants patients a right to have doctors and other health care professionals use the ePA. The PDSG stipulates that patients can insist on the storage of health care data such as medical findings, doctor's reports and radiographies in the centralised ePA. This also includes emergency data sets, medication plans and medical letters available in electronic form. From 2022, the legislator will extend this to include the vaccination card, the maternity pass, the yellow examination booklet for children and the dental bonus booklet.

A further essential regulatory content of the PDSG is patients' control over their health care data. Therefore, they will be entitled to determine in detail who can view which data - and what, for example, should not be accessible to certain doctors. Insured persons may choose to store documents individually and object to others. The legislator strengthens this self-determination by granting patients the right to deletion access restriction. Limited access can, for example, include the family doctor

and exclude a specialist. Insured persons should also be able to take the data with them when they change their health insurance company.

Moreover, the PDSG ensures transparency by giving policyholders access to all data via smartphones and tablets from 2022 onwards. Alternatively, in case they do not have access to such mobile devices, they can view their ePAs at a branch of their health insurance company. For e-prescriptions, an app will be developed with which the e-prescription can be loaded directly onto the smartphone. The patient can redeem it in a pharmacy of his choice, regardless of whether it is a local or an online pharmacy.

A further component of the PDSG is a comprehensive guarantee of data security. Every user of the telematics infrastructure - whether doctor, hospital or pharmacist - must meet high data privacy standards. If they identify deficiencies, they must report them immediately to the Company for Telematics Applications of the Health Card (gematik). Otherwise, a fine of up to 250,000 Euros may be imposed.

As a conclusion it can be said that the new PDSG is meant to significantly strengthen the rights of the insured persons. On the other hand, it also obliges insurers, hospitals and health professionals to implement the necessary processes and technology to be able to fulfil these rights.

In January 2020, the draft PDSG went into departmental coordination and is supposed to be passed by the Federal Cabinet within the next two months.

If you have any questions, please let us know

Sebastian Hoegl, LL.M. (Wellington)

Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49 761 76999-920
E: shoegl@kpmg-law.com

Dr. Ariane Loof

Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49 30 530199-625
E: aloof@kpmg-law.com

Maik Ringel

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

Nikola A. F. Werry, LL.M. (UK)

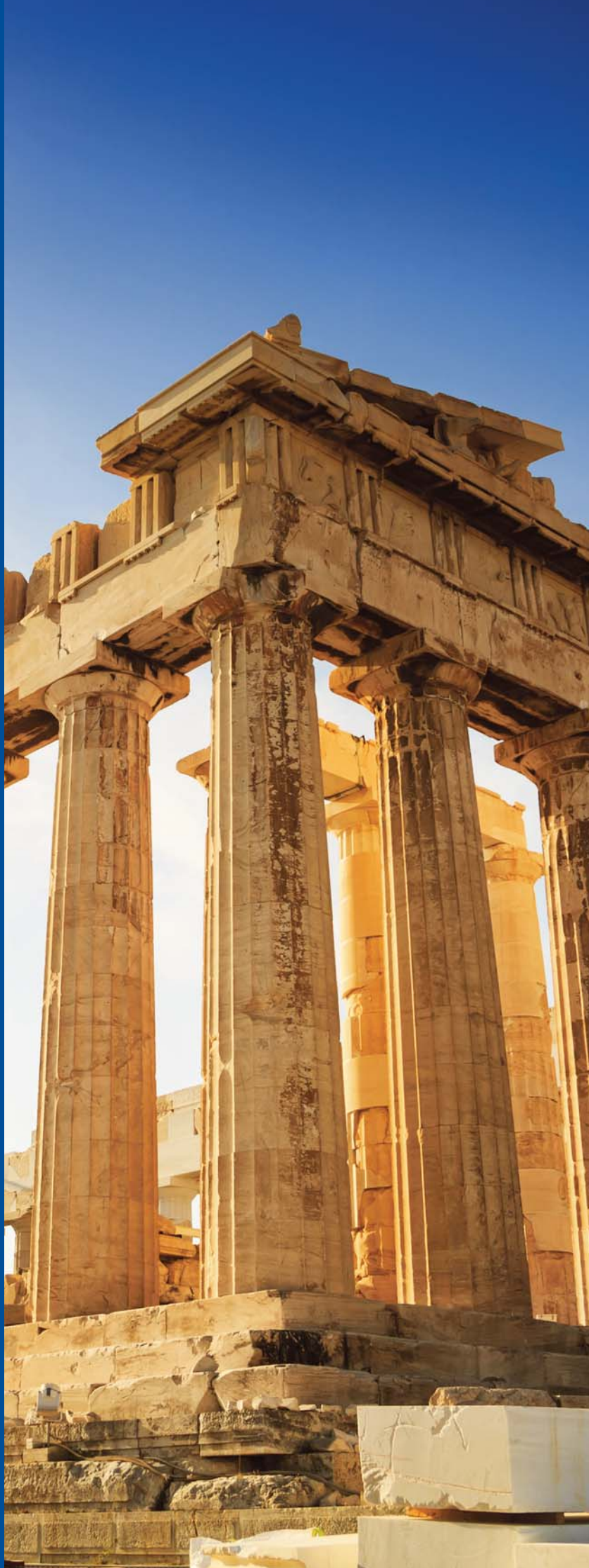
Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49 69 951195-027
E: nwerry@kpmg-law.com

Thorsten Jansen

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

Greece

- Decisions of Hellenic DPA provide for correcting measures and impose significant fines
- The Opinion of the Hellenic DPA on the Greek GDPR Law 4624/2019
- Hellenic DPA statistics (period: October 2019 to February 2020)



Decisions of Hellenic DPA provide for correcting measures and impose significant fines

– The Hellenic DPA imposed significant fines (amounting to EUR 400 000 and EUR 200 000 respectively) on **Telecommunications Companies**.

In particular, the Hellenic DPA found that GDPR provisions on data protection by design and on data accuracy have been violated. Due to a problem in the interconnection of the Company's systems, although data subjects/subscribers had exercised their "opt-out rights", following their right to data portability, they were subsequently re-registrated with the operator's registry of clients and they received calls for marketing purposes.

– The Hellenic DPA imposed fines of EUR 150 000 and EUR 15 000 to **Maritime Companies**:

- The first maritime company audited by the Hellenic DPA processed personal data in a computer infrastructure (hardware and software-server) without complying with several GDPR principles relating to the lawfulness of the processing, nor did it demonstrate accountability as required by GDPR. In addition, it violated the provisions on data retention and security of processing (in particular confidentiality) by failing to adopt appropriate techniques and organizational measures, mainly those involving the physical and reasonable separation of hardware, software and data, resulting in the company illegally copying the entire server content (back up servers). Consequently, the Hellenic DPA imposed a fine of EUR 150 000
- The second maritime company audited by the Hellenic DPA, retrieved deleted e-mails from its server within the context of an audit carried out for one of its managerial employees suspected for acting against the interest of the company. The company was in compliance with GDPR since its internal policies and regulations clearly prohibited the use of corporate electronic communications and networks for private purposes, while they also clearly mentioned the ability of the company to conduct internal audits. On the contrary, the Company's CCTV was illegally installed thus the material submitted to the Hellenic DPA was

not taken into account. Furthermore, the Company did not satisfy the employee's right of access to the personal data contained on the corporate PC he was using. The Hellenic DPA imposed a fine of EUR 15 000 on the company for illegally installing and operating a video surveillance system and for further processing of the related material.

– The Hellenic DPA issued reprimands to the Ministry of Mercantile Marine and Island Policy for infringement of the right to access: Following a complaint to the Hellenic DPA that the Ministry of did not satisfy the data subject's right of access and correction, the Hellenic DPA, after investigating the case, issued a reprimand to the Ministry of Mercantile for not satisfying the subject's right of access.

The Opinion of the Hellenic DPA on the Greek GDPR Law 4624/2019

The Hellenic DPA has issued a number of comments on the Greek Law implementing GDPR and the provisions of EU Directive 680/2016 on Personal Data and Law enforcement, 6 months after its passing through Parliament.

The main concerns of the Hellenic DPA for the provisions of the law were that:

a) The law is not compatible with GDPR in certain cases and

b) The vagueness of many important provisions may be found misleading for both the data subjects and their processors, as well as for the judicial authorities

In particular:

- The GDPR defines only the terms "controller" and "processor", whereas the local law adds two new terms: the public and the private sector.
- Regarding the ability to amend the purpose of processing by private entities, local law provides that the processing of personal data by public and private bodies for a purpose different than the one for which data has been collected is permitted in case that it is necessary, amongst other, for the avoidance of threats against national safety, following a request made by the public body or for the prosecution of criminal offences. These provisions are not compatible with GDPR nor with the principle of provision of criminal protection by the State.
- The law introduces special regulations for the processing of personal data within the framework of employment in the private and the public sector, which amongst others provide that the personal data of the employees could be submitted for processing for the purposes of the employment contract, only if absolutely necessary for the conclusion of such contract or after its conclusion, for the execution of the contract. The DPA considers that these provisions are not compatible with GDPR, because the member states could only specify the purposes of processing and not add new purposes.

– The reference of the local law on employees' consent as a basis for processing, provides for a wide base in order for the employer to justify processing on consent grounds.
– In certain articles of the local law, important deviations from the GDPR are established regarding freedom of expression and information, limiting amongst others, fundamental basic rights of data subjects, such as the right to be forgotten.

The Greek DPA reserved its right not to implement provisions of the law which are contrary to GPDR and its overall opinion seems to recommend that the law should be entirely revised.

As regards to the Directive 680/2016 implemented in Greece with the same law, the Hellenic DPA identified many issues related to the non-compliance or mistaken compliance with the rulings set out in the Directive.

Hellenic DPA statistics (period: October 2019 to February 2020)

Period from October 2019 to February 2020:

Complaints filed with DPA: 291

Breaches notified to DPA: 37 (7 referred to e-privacy breaches)

Fines imposed from May 2019 to February 2020 for GDPR violation:
EUR 715 000

If you have any questions, please let us know

Liana Kosmatou

Lawyer/Director, KPMG DPO
CPALaw
T: +30 210 60 62 159
E: lkosmatou@cpalaw.gr

Penny Vithoulka

Lawyer/Senior Manager
CPALaw
T: +30 210 60 62 159
E: pvithoulka@cpalaw.gr

Romania

- Administrative fine applied against a non-banking financial institution
- Administrative fine applied against an energy sector company
- Administrative fine applied against a shipping industry company
- Summary of the National Supervisory Authority for Personal Data processing

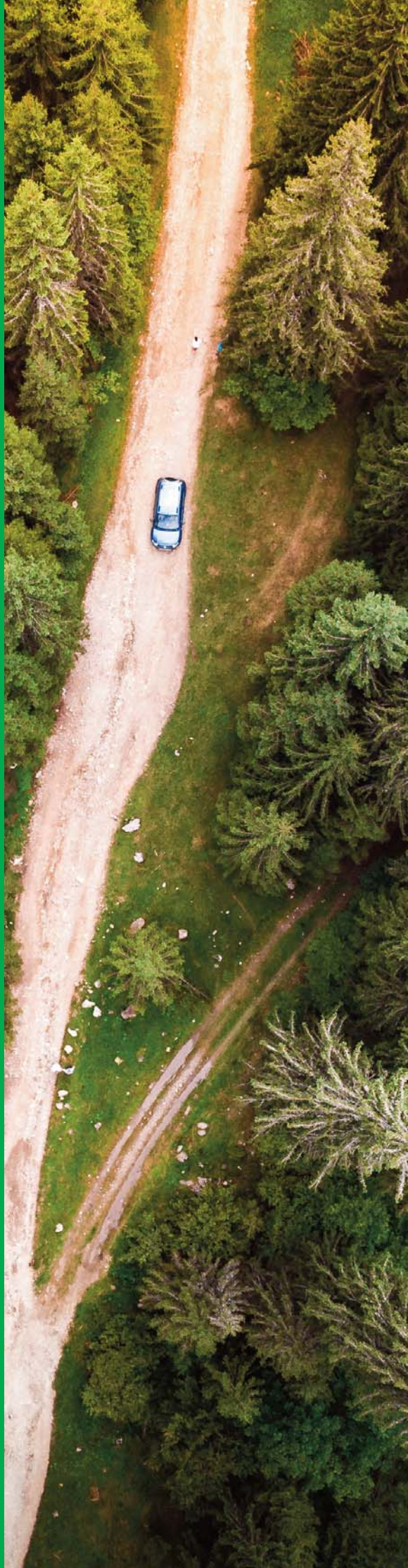
Administrative fine applied against a non-banking financial institution

On **13 January 2020**, the National Supervisory Authority for Personal Data Processing ("DPA") published a news report stating that an administrative fine of **EUR 14 000** had been applied against a non-banking financial institution, (**"Company"** and/or the **"controller"**) for non-compliance with certain provisions of GDPR (i.e. articles 5, 25, 32 and 33).

Further to the investigation, the DPA ascertained that the Company was processing personal data without proving the applicability of an efficient mechanism for the verification and validation of the accuracy of the personal data collected and subsequently processed, or to maintain its confidentiality, according to GDPR principles.

In addition, the DPA ascertained that the Company had failed to take sufficient measures for the security of personal data, in order to avoid unauthorized disclosure and access to personal data by third parties. Moreover, the controller failed to notify the authority with respect to a personal data breach within the term of 72 hours as stipulated under GDPR.

In addition to the administrative penalty, the DPA applied corrective measures against the Company, to ensure its compliance with the GDPR provisions covering operations for collecting and subsequent processing of personal data with respect to (i) accuracy of personal data, (ii) professional secrecy, (iii) confidentiality of personal data, (iv) implementation of an internal policy which is adequate for identification of risks, their analysis and notification to the authority in the case of a personal data breach.



Administrative fine applied against an energy sector company

On **14 January 2020**, the DPA published a news report stating that an administrative fine of **EUR 6 000** had been applied against a company providing electricity and natural gas, (**"Company"** and/or the **"controller"**) for non-compliance with (i) the accuracy principle, (ii) personal data processing operations on the basis of consent of the data subject and (iii) non-compliance with the data subject's right to opposition.

The administrative fine has been applied as a result of the petition lodged with the DPA by a data subject who claimed that the Company unlawfully processed his/her personal data to the extent that the controller had not had the data subject's prior consent for sending him/her notifications via his/her e-mail address and it processed the personal data without observing the accuracy principle.

In addition, the DPA ascertained that the Company had failed to take the appropriate measures to stop sending the data subject notifications, even though the latter exercised many times his/her opposition right in connection with the notifications received.

Administrative fine applied against a shipping industry company

On **16 January 2020**, the DPA published a news report stating that an administrative fine of **EUR 10 000** and **2 written warnings** had been applied against a shipping industry company (**"Company"** and/or the **"controller"**) for non-compliance with certain GDPR provisions.

The DPA applied the penalties due to the fact that:

(i) The controller did not present evidence to prove that it had provided clear, complete and correct information to the data subjects.

(ii) The controller had excessively processed the personal data (images) of its employees through the video surveillance cameras installed in the offices where they were working and in the places where there are cabinets where the employees store their spare clothes (changing rooms).

(iii) The controller processed employees' biometric data (fingerprints), while other means could be used so as to achieve the purpose set out by the employer, which would have been less intrusive for the privacy of the data subjects.

(iv) The controller illegally processed the personal data of a former employee by using it in correspondence through electronic e-mail, in order to carry out the activity of the company, after the termination of the contractual relationship with the employee.

Further to the completion of the investigation, the DPA ascertained that:

(i) The controller did not prove a justified legitimate interest for performing the surveillance, did not prove consultation with the trade union/ representatives of the employees before the introduction of the monitoring systems, and, moreover, had not effectively demonstrated that other less intrusive forms and methods for achieving the employer's purpose had been tried and found to be ineffective.

(ii) The controller did not prove the existence of adequate data protection policies nor the implementation of adequate technical and organizational measures to ensure a level of security appropriate to this risk.

(iii) The biometric data processed through the access control system was not collected for appropriate purposes, and was not relevant and limited to what was necessary in relation to the purposes for which they were processed.

(iv) The controller did not carry out a personal data impact assessment.

In addition to the written warnings and administrative fines, the DPA also applied certain corrective measures against the Company (e.g. to ensure the correct data subjects' information by communicating in a concise, transparent, intelligible and easily accessible form all the information, as set out in art. 13 GDPR and under the conditions of transparency mentioned in art. 12 of GDPR, as well as to modify the documents by means of which the data subject is currently informed; to ensure the compliance of personal data processing operations within video monitoring activities etc.).

Summary of the National Supervisory Authority for Personal Data processing

Brief summary of the most significant aspects of the activity of National Supervisory Authority for Personal Data Processing (the **"Romanian DPA"**) during 2019, as follows:

(i) in 2019, the National Supervisory Authority received a total of **6 193** complaints, intimations and notifications concerning the personal data breaches, based on which **912 investigations** were opened;

(ii) as a result of the investigations conducted, **28 fines** having a total amount of **RON 2 339 291.75** were imposed;

(iii) a number of **134** written warnings and **128** corrective measures were imposed;

(iv) regarding the activity of handling the complaints, the Romanian DPA received a total number of **5 808 complaints**, on the basis of which **527 investigations** were initiated;

(v) as regards the personal data breaches, the controllers submitted, both under the GDPR and Law no. 506/2004 regarding the processing of personal data and protection of private life within the electronic communication sector, a number of **233 notifications**, and a number of **152** intimations regarding possible non-compliance with the provision of the GDPR was received;

(vi) in the context of cooperation with other supervisory authorities in order to ensure mutual assistance, about **30** requests were handled regarding the application and enforcement of GDPR;

(vii) concerning the activity of representation before the courts of law, the Romanian DPA managed a number of **207** files that are pending on the dockets of the competent courts;

(viii) throughout 2019, controllers have continued to declare before the Romanian DPA the **data protection officers** appointed, registering with the Romanian DPA a number of **4 318** officers (appointed both in the public and private sector).

If you have any questions, please let us know

Cristiana Fernbach

Partner, KPMG Legal
KPMG Legal acts in Romania through Toncescu si Asociatii
T: +40 372 377 800
F: +40 372 377 700
M: +40 722 779 893
E: cfernbach@kpmg.com

Spain

- The Spanish authorities publish a guide on AI
- Instruction 2/2019 of the State Public Prosecutor's Office on the protection of personal data was published
- Trend of the Spanish Data Protection Authority in its sanctioning activity since the date of application of the GDPR
- The Spanish Data Protection Authority presents a campaign to prevent the disclosure of sexual or violent content on the Internet through its Priority Channel

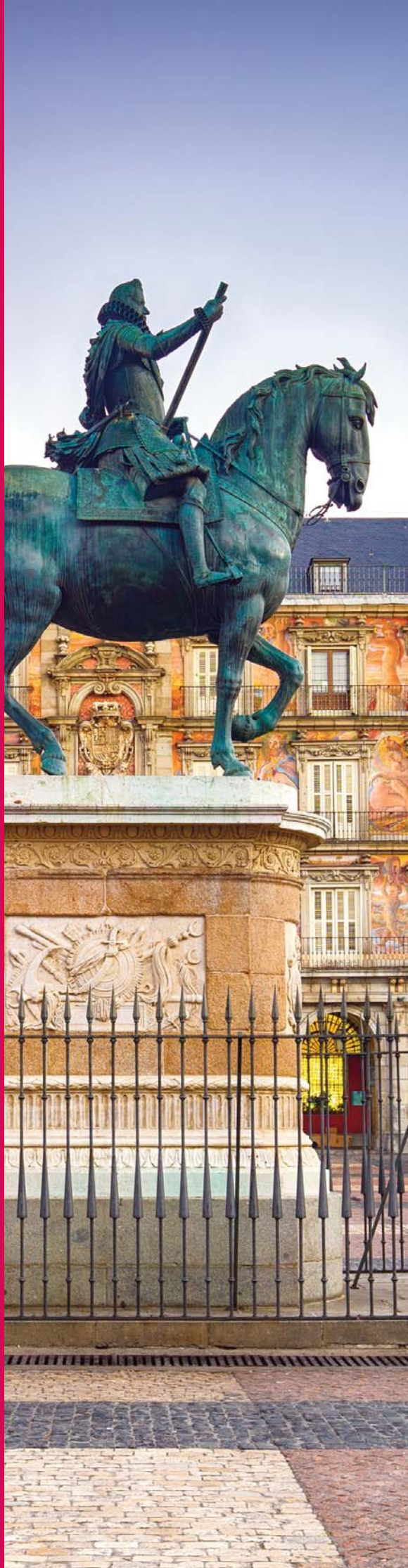
The Spanish Authorities publish a Guide on AI

Last 13 January 2020, the Spanish Data Protection Commissioner ("AEPD" in its Spanish acronym) published on its website the guide "Adequacy of processing activities incorporating Artificial Intelligence to the GDPR. An introduction". A first approximation for the adequacy to the GDPR of products and services that include Artificial Intelligence components.

The guide provides a straightforward overview on some of the technical attributes, and the data protection regulatory aspects, of AI systems, providing directions on major regulatory issues regarding the use of these types of technologies.

Concerning **accountability**, the authorities clarify that the adopter of an AI solution cannot hide behind a lack of information or technical knowledge in order to avoid his responsibility when it comes to auditing and deciding whether the system is GDPR compliant. Transferring the responsibility to the developer/supplier of the tool, lesser to the AI system itself, is not an option in the eyes of the AEPD. Although the AEPD recognizes that when AI goes from being an experimental element to a product, it would be advisable to introduce certification systems and protection marks, when approaching a product or service based on AI, it is the user (the client) who has the duty to audit the processing activities that will take arise from such use. A call for attention to both users and developers, who, however, are not exempt from responsibility towards their clients if their systems are not privacy respectful.

With regard to the **duty to inform**, the AEPD clarifies that information must be provided to enable the behaviour of the processing to be understood. Although it will depend on the type of IA component used, the AEPD provides an example of the level of detail to be provided; a word of warning for both developers and users who should provide details on the processing such as (i) the data used for decision making, (ii) the relative importance that they have in decision making, (iii) the quality of the training data and the type of patterns used, among others. In other words, much more detailed information than that usually included in the privacy notices of these types of tools.



The guide also reviews all **data protection rights** and clarifies that it will be necessary to include an effective information governance model, allowing traceability of the information in order to identify the controller and enabling the exercise of the data protection rights, including the duty to block the data.

The AEPD expressly establishes that the data collected for training purposes must be purged of all information not strictly necessary for carrying out such activity (training the model). Likewise, it refers to its application at the time of distribution, and provides a catalogue of different **data minimisation** techniques for Artificial Intelligence applications, some specific for ML. We miss in this section perhaps some reflection on more advanced AI systems, based on neural networks that learn automatically when they are provided with huge volumes of information.

The guide goes over many other topics, providing clarity and boundaries for all the stakeholders (developers, users and data subjects). Indeed, a necessary document. We look forward to the AEPD's "Chapter 1".

Instruction 2/2019 of the State Public Prosecutor's Office on the protection of personal data was published

The instruction analyses the position of the Public Prosecutor's Office as data controller, the data protection obligations applicable to its activity and the role of the Data Protection Officer (DPO).

The activity of the Public Prosecutor's Office (hereinafter, PPO) involves the processing of personal data which must comply with the applicable regulations. This activity is developed fundamentally in the context of the jurisdictional activity related to the fulfillment of its duty of promoting the action of justice in defense of legality, the rights of citizens and the public interest.

Therefore, the PPO determines the need to assume responsibility for compliance with data protection regulations, to identify which obligations applicable to all entities that process data must be fulfilled by the PPO and how data subjects must be assisted in exercising their rights.

It is also anticipated that the Chief Public Prosecutor will request the appointment of a DPO to be chosen from among all the prosecutors, who will be assisted by a team of deputies in the performance of his duties.

It should be noted that the PPO is subject to a special sanctioning regime applicable to constitutional bodies. This regime establishes that when they infringe the data protection regulations, the competent authority will issue a ruling in the form of a warning without a financial penalty, notwithstanding application of the general regulations on civil, criminal and disciplinary liability that may be applicable.

Trend of the Spanish Data Protection Commissioner in its sanctioning activity since the date of application of the GDPR

The General Regulation on Data Protection (GDPR) has meant a substantial regulatory change, introducing novelties both in the rights of citizens and in the way in which personal data are processed by organisations. Therefore, the Spanish Data Protection Commissioner (AEPD in its Spanish acronym) has also had to prepare itself for the transition from the previous legislative framework to the GDPR, in addition to the approval of Constitutional Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights in December 2018, which supplements and construes some provisions of the GDPR.

Since May 25 2018, the AEPD has focused its activity on publishing different materials such as guidelines and legal reports to promote and facilitate the adaptation of companies to the new regulations, interpreting their provisions and guiding data controllers and processors in its implementation. But a year and a half after the GDPR is applicable, the AEPD is beginning to make use of its sanctioning powers and investigate those entities that have not adapted their practice to the applicable regulations.

Spain

Since 2018, the AEPD has issued 54 sanction resolutions to private entities. With regard to the matter of the sanctioning procedures, the following are of particular relevance: fraudulent contracting, undue insertion in credit information systems, video-surveillance, spam, advertising, internet services, debt claims and telecommunications. The highest sanctions imposed so far are as follows:

- EUR 250 000 to the Spanish Football League for the use of an app that uses the mobile microphone to fight against football piracy without providing clear information, consisting of an infringement of Article 5.1 (a) of the GDPR for breach of the principle of transparency.
- EUR 75 000 to a telecommunications operator. The data subject, a former customer of the company, continued to receive invoice notifications, although at that time there was neither a contractual relationship nor any payment overdue from the expired contractual relationship. As a reason for the incorrect mailings the entity indicated a technical error.
- EUR 60 000 to a telecommunications operator for the unlawful processing of data, including bank details, customer address and name of the data subjects.

Although the fines are not always particularly high, in terms of volume, the Spanish data protection authority is rapidly increasing its activity around the implementation of the GDPR.

The Spanish Data Protection Commissioner presents a campaign to prevent the disclosure of sexual or violent content on the Internet through its Priority Channel

The Spanish Data Protection Commissioner (AEPD in its Spanish acronym) launched a campaign aimed at promoting the use of its Priority Channel to report sexual or violent content published on the Internet without the permission of the people who appear on it.

The purpose of the AEPD's Priority Channel is to provide a means of communicating the illegal disclosure of sensitive content and requesting its withdrawal, offering a rapid response in exceptionally sensitive situations.

Once the complaint has been filed through the channel, the AEPD will analyse the claim and determine the urgent adoption of the precautionary measures provided for in the Spanish Data Protection Law. This would prevent the continuation of the unlawful processing of personal data in particularly serious cases such as victims of gender violence, abuse or sexual assault or harassment, or any other particularly vulnerable group such as minors, persons discriminated on the basis of their sexual orientation or race, persons with disabilities or serious illness or at risk of social exclusion.

Furthermore, the AEPD will assess whether it is appropriate to initiate sanctioning proceedings against the persons who have disclosed such material.

If you have any questions, please let us know

Bartolomé Martín

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

Claire Murphy

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

Turkey

- Extension for VERBİS
- Data Breach Notifications Published by the Turkish DPA
- Complaints to the Turkish DPA
- Data Breach Notifications via Electronic Means

Extension for VERBİS

The Personal Data Protection Board ("Turkish DPA") extended the deadline of Data Controllers Registry Information System ("VERBİS") registration.

Pursuant to Article 16 of the Law on Personal Data Protection No. 6698 ("KVKK"), real and legal persons who process personal data must register with the Data Controllers Registry before starting any data processing.

The deadline which was initially announced as 03.09.2019 and had been extended to 31.12.2019. This time the Turkish DPA, with its decision dated 27.12.2019, numbered 2019/387 announced a third extension of the VERBİS registration requirement.

New Deadlines to Register to VERBİS

Data Controllers	Deadline
Data Controllers with more than 50 employees annually or an annual financial balance of more than TL 25 million	30.06.2020
Data Controllers residing or registered abroad	30.06.2020
Data Controllers whose main business activity is processing special categories of personal data but with less than 50 employees or a total financial balance of less than TL 25 million	30.09.2020
Data Controllers that are public institutions and organizations	31.12.2020

The Turkish DPA has taken this decision considering that most of the registrations and notifications failed to satisfy the main purpose of the VERBİS. According to the Turkish DPA, the purpose is not only to register but also to keep the data inventory up-to-date and to provide accurate, transparent and accountable data processing activities.

The Turkish DPA particularly stated that the VERBİS notifications should be made on the basis of the personal data inventory prepared within the scope of the processes within the organization of the data controller, and that such processes should be parallel to those that appear in VERBİS.

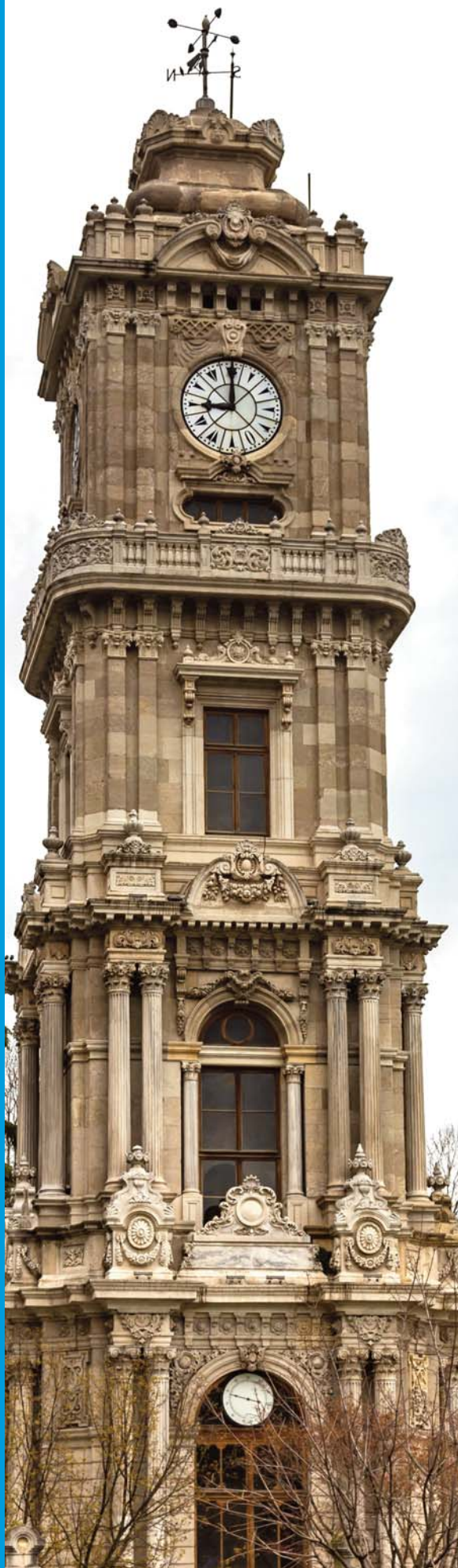
The Turkish DPA also stated that as a result of its evaluation over VERBİS; some data controllers assumed that they had fulfilled their obligation to register by only submitting the pre-application forms to the Turkish DPA. The Turkish DPA has pointed out that the notification should be completed by pressing the "Confirm and Submit" button; otherwise, the obligation to register and report to VERBIS will not be deemed fulfilled.

Data Breach Notifications Published by the Turkish DPA

Article 12(5) of KVKK sets forth that a data controller must notify the data subject and the Turkish DPA within 72 hours if any processed data is obtained by other parties via unlawful methods. Where necessary, the Turkish DPA is entitled to announce such breaches on its official website or through other methods it deems appropriate.

In this direction, the Turkish DPA has published 43 data breach notifications on its official website. These notifications include data controllers such as banks, hotels, software and pharmaceutical companies as well as various retail companies. The most recent notification published on the official website is related to a data breach that occurred in Microsoft Corporation; which states the following;

- The breach occurred between 05.12.2019 and 31.12.2019 and detected on 26.01.2020,
- The breach occurred due to the accessibility of a database containing information on Microsoft support service representatives' interactions with customers via the internet as a result of incorrect configuration of the security rules,
- The categories of personal data affected by the breach are communication, customer transaction, transaction security, and financial data,
- The estimated number of people affected by the breach is 158 users in Turkey,
- Further information about the data breach is available on the Microsoft website.



Complaints to the Turkish DPA

Article 15 of KVKK sets forth that the Turkish DPA shall carry out the necessary examination upon complaints or ex officio once it becomes aware of an alleged infringement. The Turkish DPA launched a "KVKK Complaint Module" as of 09.01.2020 to enable the public to submit complaints easily and effectively.

Data Breach Notifications via Electronic Means

Within the context of data controllers' responsibility to protect the personal data against unlawful processing, illegal access, and the duty to notify the Turkish DPA of any breaches in this regard, the Turkish DPA has published a Personal Data Violation Notification Template and decided that such notifications may also be submitted via the website link.

If you have any questions, please let us know

Onur Küçük

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

UK

- First UK GDPR fine imposed, and other enforcement news
- Brexit
- Artificial Intelligence
- Automated Facial Recognition

We have selected a few items on the activities of the UK regulator, the Information Commissioner's Office (ICO) in recent months.

First UK GDPR fine imposed, and other enforcement news

The ICO has imposed its first fine under the GDPR. It fined a pharmacy £275 000 for failing to ensure the security of special category data. 500 000 documents containing customer details (including names, dates of birth and medical information) were left in unlocked containers outside the back of the pharmacy's premises in Edgware, London. The business' data protection policies were also found to be wholly inadequate, with large sections referring to legislation predating the GDPR.

Due to the multiple breaches of the GDPR committed, the ICO issued an enforcement notice in addition to the fine. The pharmacy will have to comply with specific requirements, including updating its data protection policies and making its staff aware of their obligations, within three months.

The ICO considered the breach "extremely serious" and that it demonstrated a "cavalier attitude to data protection". However, in assessing the amount of the fine, she took into account the size of the pharmacy and the information available to her about its financial position, acknowledging that the fine must be effective, proportionate and dissuasive.

In GDPR terms, this fine appears relatively small, but the ICO demonstrated an appetite to use its powers to the full just a few weeks later. A fine of £500 000 was imposed on a nationwide retailer in respect of security breaches that had occurred prior to GDPR coming into force. The fine is the maximum amount possible under the pre GDPR legislation. The ICO commented that "but for the statutory limitation on the amount of the penalty, it would have been reasonable and proportionate to impose a higher penalty" said that if it had not been for the statutory limit, a greater fine would have been imposed.

Meanwhile, following the notices of intent issued last summer to fine a two organisations sums in the millions under GDPR, fines have not been imposed. It is understood that the period for the regulatory process has been extended.

Brexit

The UK left the European Union on 31st January 2020 and entered into a transitional period that will end on 31st December 2020.

On 29th January 2020, the ICO issued a statement confirming that during the transitional period the GDPR would continue to apply, and that it is "business as usual". She also confirmed that:

– The ICO will continue to act as the lead supervisory authority for businesses and organisations operating in the UK.

– Companies and organisations who offer goods or services to people in the EU do not need to appoint a European representative during the transition period.

The ICO recognised that the future looks uncertain on the Data Protection landscape, in particular in relation to data flows, but confirmed that they will be monitoring the situation and updating its external guidance accordingly. Organisations are taking steps to ensure that personal data will be able to flow between the UK and Europe at the end of the transition period.

Artificial Intelligence

Artificial Intelligence ("AI") is a key area of focus for the ICO. Building AI involves creating an algorithm from data to model some aspect of the world. The model is then applied to new data in order to make predictions. Advances in technology mean that the creation of AI is increasingly automated. The calculations and processes used by AI to arrive at conclusions can be difficult to understand, and those affected by AI-generated decisions may not be able to hold anyone accountable for the consequences that they suffer. ICO research shows that over 50% of people are concerned about machines making complex automated decisions about them.

In response to these concerns, the ICO and the Alan Turing Institute (the UK's national institute for data science and AI) have collaborated to produce draft regulatory guidance on the use of AI. The draft guidance proposed the following key principles for those developing AI based decision-making systems:

1. **Transparency:** make use of AI for decision-making obvious and appropriately explain the decisions made to individuals in a meaningful way.
2. **Accountability:** ensure appropriate oversight of the AI decision systems, and be answerable to others.
3. **Consider Context:** there is no one-size-fits-all approach to explaining AI-assisted decisions.
4. **Reflect upon its impact:** ask and answer questions about the ethical purposes and objectives of the AI project at the initial stages of formulating the problem and defining the outcome.

Where an individual would in the past have been able to expect an explanation from a human, they should in future be entitled to expect an explanation from those accountable for an AI system. The consultation on the draft closed in January and the final guidance is awaited.

Automated Facial Recognition

Automated Facial Recognition ("AFR") continues to be a high priority for the ICO. We understand that several investigations are ongoing.

In October 2019, following conclusion of investigations into police use of AFR in public places, the ICO issued an Opinion on the subject. It found that there was public support for use of the technology, but that there needed to be improvements in how the police authorised and deployed the technology if it is to retain public confidence and address privacy concerns.

The Opinion confirmed that:

- Whether the technology is being used on a trial basis or as part of a routine operation, its use is subject to Data Protection laws. A lawful basis must be identified, a Data Protection Impact Assessment must be undertaken and an appropriate policy put in place.
- It must be demonstrable that that each use of AFR is strictly necessary (taking into account proportionality). The effectiveness of the technology in achieving a demonstrable public benefit must be clearly explained.
- Any use of AFR by police forces would be considered "sensitive processing" as it uses biometric data to identify individuals. This is taken to occur irrespective of whether or not the image captured yields a match to any criminal database, or where unmatched data is only kept for a very short time.

The Opinion followed the widely reported Bridges case in which the use of AFR by the South Wales Police had been challenged. The court had concluded that the use of AFR complied with Data Protection laws, however, the ICO has emphasised that the judgment should not be taken as a blanket authorisation for the police to use AFR. The ICO intends to work with relevant authorities to strengthen the legal framework in this area and provide further guidance.

Whilst public support for use of AFR by the police to catch criminals has been found to be high, the ICO has found that there is less support for its use by the private sector in a quasi-law enforcement capacity or when used in partnership with law enforcement authorities, and intends to report on this further in due course.

If you have any questions, please let us know

Isabel Ost

Solicitor/Director/Legal Services - Data Protection
KPMG in the UK
M: +44 (0)7818 588 789
T: +44 (0)207 694 3361

Lucy Jenkinson

Solicitor (England and Wales)/Senior Manager/Legal Services - Commercial
KPMG in the UK
Direct Line: +44 (0) 131 527 6823
M: +44 (0) 7825 089364