KPMG

# Data privacy newsletter

**KPMG Global Legal Services**

December 2019

# Contents

# Introduction

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

As the second year end celebration with the GDPR in force looms, various jurisdictions have significant and interesting news. The national courts are getting more and more involved and the Data Protection Authorities are strengthening their efforts. The Court of Justice of the European Union has issued 4 significant decisions with regard to data privacy that have global impact.

The authorities from Spain have published guidelines on Privacy by Design (as has the European Data Protection Board and the German authorities) and on the use of cookies. In that last guideline, they have taken a view different from the view of the Court of Justice of the European Union. Bulgaria reports a decision by its authority with regard to the handling of employee data and a decision by Bulgaria's Constitutional Court. The Czech Republic has made new experiences with how the courts handle the demand for damages once data privacy laws are violated. Additionally, there are new developments with regard to commercial communication and the reporting of data breaches.

The Italian authorities have started investigating about 100 companies on their compliance with data privacy news. Germany has handed out its first 8-digit fine and the German authorities have agreed – may it be a coincidence or not – on a model how to calculate fine. They plan to bring that model to the European Data Protection Board for further evaluation and discussion.

Russia, while not being subject to the GDPR, is contemplating a law which would fine companies if they do not comply with an already existing law from 2015 which makes it requirement to store data of Russian citizens in Russia.

In news from the European Data Protection Board you can read on their concern regarding international data transfer and their take on Data Protection by Design and by Default as well as the territorial scope of the GDPR.

And last but not least: while we hope that you enjoy our third issue of our Data Privacy Newsletter, we hope even more that you and your loved ones enjoy all the warmth this season has to offer.

# International

## European Data Protection Board adopts Guidelines on Data Protection by Design and by Default and on the territorial scope of the GDPR

In its 15th Plenary session in November 2019, the European Data Protection Board adopted guidelines on Data Protection by Design and by Default and on the territorial scope of the GDPR. In the guideline on Data Protection by Design and by Default, the board points out the utter importance of the concept of Data Protection by Design and by Default for the promotion of privacy and data protection in our society. The Board concludes that the effective implementation of the principles and rights of data subjects is the main objective. The Board has therefore issued numerous detailed recommendations, aimed at controllers and technology providers alike.

Additionally, the Board specified in the Guideline on the territorial scope of the GDPR when the GDPR applies on controllers and processors inside and outside of the European Union. Using numerous examples, the guideline goes into very much detail in assessing the applicability of the GDPR. It especially deals with the question when a controller or processor is established in the European Union. It also provides detailed examples on the question when the GDPR applies to controllers and processors established outside of the European Union on the basis that data subjects in the European Union are targeted by their offerings.

## European Data Protection Board voices concern on the EU-U.S. Privacy Shield

Also in its 15th Plenary session in November 2019, the European Data Protection Board has issued its third Annual Joint Review on the EU-U.S. Privacy Shield. The EU-U.S. Privacy Shield is meant to provide an instrument that protects personal data according to European standards when it is transferred to (or accessed from) the United States. While the Board expressly welcomes the efforts made by the EU Commission and the US authorities, it still sees numerous areas that need further addressing. Those areas include the requirements regarding onward transfers, HR data and the application of the principles when it comes to processors, as well as the recertification process. One area of concern is also the collection of data by public authorities. The Board emphasized that the same concerns will be addressed by the Court of Justice of the European Union in pending cases.

# International

## The CJEU rules in the Planet49 Case regarding the use of cookies on websites

In its ruling, the Court of Justice of the European Union (CJEU) has finally rejected the so-called "opt-out" for tracking cookies. One of the core statements of the judgement is: "Silence, boxes already ticked or inactivity" cannot constitute consent, as this must be actively given within the framework of an "opt-in". In its decision, the court also clarified that, among other things, information on the duration of the cookies' function and access by third parties belong in the data subject information. The requirements of the CJEU and the GDPR for effective consent and the interests as a website operator are difficult to reconcile in practice. Website operators who do not completely dispense with tracking cookies and still wish to comply with data protection regulations will need complex cookie banners or other content solutions.

## Further Decisions by the CJEU

In addition to the aforementioned decision, the CJEU has issued more decisions with regard to data privacy. The CJEU has held that search engine operators are not required to de-reference links regarding a data subject on a global basis. In a different case regarding search engine operators the Court held that a search engine operator must weigh the rights of individuals requesting the removal of their sensitive information against the freedom of information of Internet users, in order to determine whether to remove such information. And in another decision the CJEU held that a court of an EU member state could order a host provider to block access to information covered by an injunction on a global basis.

# Bulgaria

A. Decision by the Commission for Personal Data Protection on correspondence regarding employee data

B. Decision by the Commission for Personal Data Protection on copying driver licenses

C. Processing of biometric data of bank clients for administering requests

D. Constitutional Court rules on balance between the freedom of expression and information and the right to protection of personal data

# A. Decision by the Commission for Personal Data Protection on correspondence regarding employee datas

**Current and former employers are not entitled to exchange information on the social security status of individuals who served as their employees.**

The Commission for Personal Data Protection (CPDP) published a decision concerning a case where the current employer of an individual, entitled to a state pension, contacted his former employers. The latter were contacted with a request to provide information on the social security status of the individual who was employed by them in the past.

According to Bulgarian legislation, the application and supporting documents for state pension must be submitted to the National Social Security Institute on behalf of the individual by the data controller who acts as employer as at the time when the individual becomes entitled to a state pension. In order to complete the set of documents, the latter requested the previous employers to issue specific certificates concerning the length of contributory service of the individual (UP-3 Certificate).

The CPDP ruled that the current employer is not entitled or obliged by law to contact the former employers with the request to issue these certificates. Consequently, the CPDP ruled that the personal data of the individual was processed without a valid legal ground.

The CPDP also stated that the answering of the request by the former employers was not compliant. Although the former employers are entitled to store information on the social security status of the individual, they were not allowed to share that information with the current employer. Therefore, the personal data of the employee was processed in violation of the purpose limitation principle.

Despite the fact that the individual concerned did not suffer any harm or damage, all three controllers were fined by the CPDP.

# B. Decision by the Commission for Personal Data Protection on copying driver licenses

**Data controllers are entitled to store a copy of the driving license of employees who perform functions related to vehicle transportation. The applicable legal ground is compliance with legal obligations.**

The Commission for Personal Data Protection (CPDP) published a statement concerning the entitlement of employers to make and store copies of driving licenses and other related documents of their employees.

Within the statement, the CPDP reminds that copies of driving licenses may be produced only if this is provided for by law. It is further explained that, for the purposes of constituting employment relationships, the employer is entitled to copy and store copies of driving licenses, if the job position must be only occupied by a licensed individual.

Furthermore, the CPDP acknowledges that in accordance with the special regulations of the transport business and traffic regulations in general, controllers should at any time be able to provide evidence that their vehicles are under the control of licensed individuals.

In conclusion, the CPDP states that controllers are entitled to store a copy of driving licenses of their employees who perform functions related to vehicle transportation for the purpose of the employment relations. Outside this scenario, data controllers may copy driving licenses in order to comply with specific legal obligations as provided in the legislative acts governing transportation business and traffic regulations. In these cases, the documents shall be copied and presented to competent authorities for the purposes of the specific inspection. Upon completion of the administrative procedure the copies should be deleted so as to comply with data minimization principle.

The statement specifically concerns making copies of driving licenses in the employment context. It does not cover making copies of driving licenses of managing directors or employees when a vehicle is provided for representation activities or as a social benefit. However, given the principle positions outlined in the traffic regulation act, we may presume that the documents in question may be copied and presented to competent authorities for the purposes of a specific inspection or another administrative procedure.

# C. Processing of biometric data of bank clients for administering requests

**The Commission for Personal Data Protection allowed the introduction of a system for voice recognition called VoiceBiometrics by a Bulgarian bank, provided that several specific requirements are met. The system will be utilized to facilitate the management, use and subscription for bank services, including the provision of information on balance and transactions history over the phone.**

The Commission for Personal Data Protection (CPDP) issued a statement with analysis of the case and ruled that the system for voice recognition may be implemented if certain conditions and requirements are complied with. These conditions and requirements concern securing conformity with all data processing and protection principles such as: lawfulness, fairness and transparency; purpose limitation; privacy by design and by default.

The statement provides that the introduction of the voice recognition system for the purpose of client support and provision of banking services, which require the identification of the particular client, is allowed if the following conditions are met:

1. The client provided his/her explicit consent for use of voice biometrics in its essence as biometric data used solely for the identification of the client, i.e. sensitive personal information. Prior to granting consent clients must be duly informed of the purposes, manner and risks related to processing, as well as for the consequences of not providing consent in compliance with the GDPR;

2. Clients must be provided with the opportunity to choose alternative identification methods which do not relate to biometrics. Otherwise, consent would not be freely given.

Furthermore, the controller is obliged to conduct a Data Processing Impact Assessment to evaluate the effect of the intended processing activities on the privacy of the bank's clients. This is due to the fact that VoiceBiometrics comprises a new technology and its scope, context and purposes may lead to a high risk for the privacy of individuals.

To conclude, the CPDP also held that in the course of introducing and implementation of the voice recognition system, the bank must comply with all requirements provided for in the primary and subordinate legislation in the field of banking.

# D. Constitutional Court rules on balance between the freedom of expression and information and the right to protection of personal data

**The Constitutional Court proclaimed that the provisions of the Personal Data Protection Act aiming to reconcile the freedom of journalistic expression and information with the right to protection of personal data are not in conformity with the Constitution.**

Back in March, the Constitutional Court was referred to examine the consonance of the amended Personal Data Protection Act rules setting a non-exhaustive list of criteria to be considered when assessing whether disclosure of personal data within a journalistic survey is in line with the right to protection of personal data, such as whether the individual is a public figure, the nature of the personal data, the necessity of the disclosure for the revealing matters of public interest, etc. (For further details on the backstory, please refer to our June edition). On the grounds of conflict with the principle for rule of law, the Constitutional Court proclaimed that the criteria set by the legislature are non-compliant with the Constitution. Upon promulgation of the judgement and following the expiry of vocatio legis period, the criteria will become inapplicable in court and by supervisory authorities.

The underlying arguments for the ruling of the Constitutional Court include:
- Being ambiguous and unclear, the formulated criteria cannot be properly construed, which may lead to self-censorship
- The formulated criteria may deprive judges of the ability to assess all relevant facts of each separate case due to over-relying on the statutory provided criteria and may provoke incoherent administrative and court practice
- The criteria impose unnecessary and disproportionate limitations on the freedom of journalistic expression

The judgement was not accepted unanimously as several judges provided a dissenting opinion arguing in favor of the challenged provision. Once the judgement enters into force, any court proceedings that were stayed awaiting resolution of the matter will be renewed. Judges hearing the respective cases, e.g. for appeal against acts of the Commission for Personal Data Protection, will be obliged to disregard the ten criteria provided by the Personal Data Protection Act.

# If you have any questions, please let us know


**Juliana Mateeva**

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

**Petya Yordanova-Staneva**

Manager, Legal Advisory, CIPP/E,CIPM
KPMG in Bulgaria
+35929697600
pstaneva@kpmg.com

**Teodor Mihalev**

Lawyer
KPMG in Bulgaria
+35929697600
tmihalev@kpmg.com

# Czech Republic

A. Monetary Compensation for Data Breach

B. Inspections overview for the first half of 2019

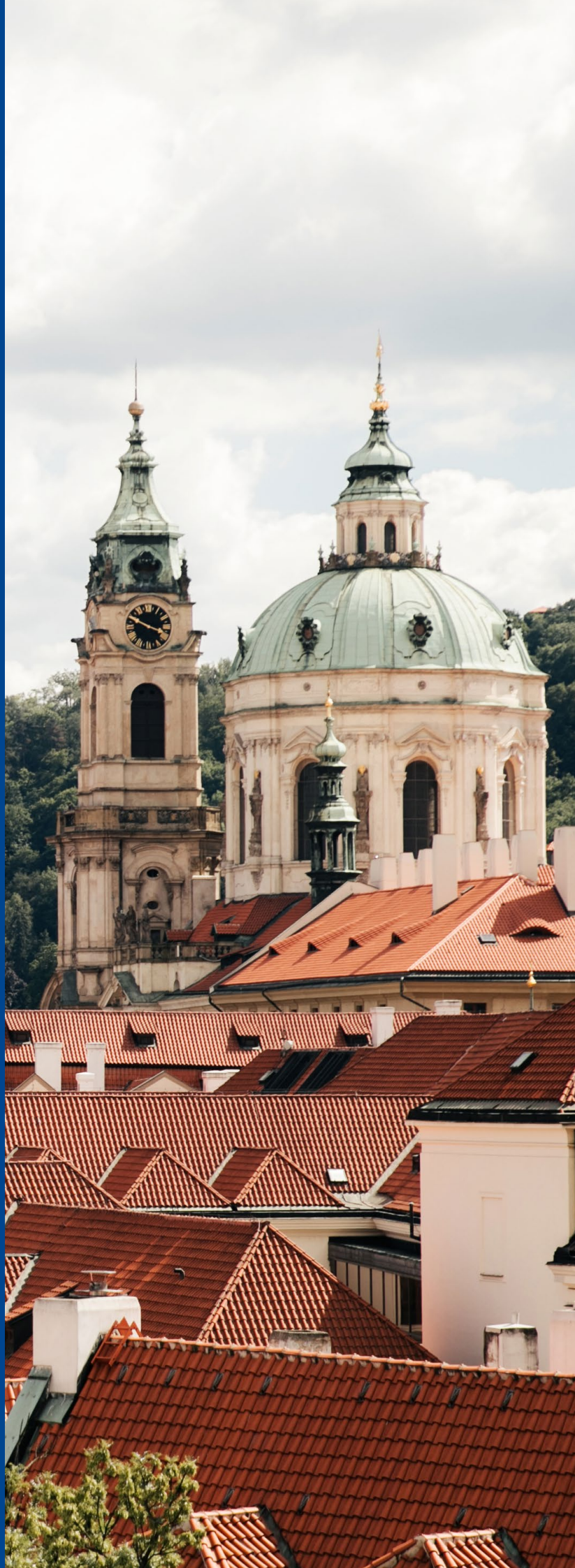
C. Unsolicited commercial communications

D. Reporting of personal data breaches

E. Second instance decisions of the Office published

F. Data Protection Impact Assessment methodology published for public discussion

G. "Banking identity" could be used in the communication with the state



# A. Monetary Compensation for Data Breach

**The Prague court has issued a resolution in the case of big personal data breach. The court ruled that the online provider who failed to meet its obligation to protect the data can be held liable and its customer can be awarded appropriate compensation. Such resolution could encourage other customers who were affected by the data breach to file actions against the provider.**

The Municipal Court in Prague considered the case concerning circa 730,000 e-mail addresses and 760,000 passwords leaked from an online shopping portal that occurred before the GDPR came into effect. Someone posted the data on one famous Czech hosting server, where it was available to anyone for about a month.

An affected costumer sued the shopping portal and claimed that the provider infringed his right against unauthorized disclosure and other misuse of his personal data. The court held that the provider indeed infringed the plaintiff's rights and that it failed to fulfil its obligations set forth by the Czech Data Privacy Act. The customer was awarded compensation of CZK 10,000 (app. EUR 400) and the provider also has to bear the costs of the court proceedings.

The court based its decision on the so-called right to informational self-determination. This constitutional right means that every person should have the right to freely decide when, where, how and which private information about such person can be made public.

This decision is the first of its kind in the Czech Republic and with upcoming class-action regulations may act as encouragement to other affected customers or even for class-action investors.

We can expect that such actions will be even more common in the future, as the GDPR expressly sets forth that any person who has suffered material or non-material damage as a result of an infringement of GDPR has the right to receive compensation from the controller or processor for the damage suffered. In this context, private claims for damages may in some instances be even more harmful for the enterpreneurs than the GDPR sanctions imposed by the data protection authorities.

# B. Inspections overview for the first half of 2019

**The Personal Data Protection Office (hereinafter the "Office") published an overview of inspections carried out in the first half of 2019. It includes reports of all cases which the Office's inspectors dealt with during this period, including a brief summary of how they decided.**

There are several cases from both the state administration and the private sector. Below please find a brief summary of some of them:

**Sales of goods and services**
- In this area, the Office dealt mainly with the processing of personal data in connection with the offer of services, approaching potential customers, and the collection, storage, transfer and erasure of personal data (retention policy). Furthermore, the Office focused on the matter whether the rights of the data subjects were respected, especially in the context of transparency and compliance with the disclosure obligations and the rights of access, rectification and erasure of personal data and the right to object.

**Marketing**
- The Office pointed out that the purchase of a database containing personal data from unknown sources is illegal. The Office imposed a fine of CZK 400,000 (app. EUR 16,000) on an inspected entity for the absence of a legal title for processing in connection with the acquisition of a contact data database.

**Employers**
- Employer's access to former employees' e-mail boxes without their consent is generally not permitted. If the employee no longer works for the company, it is advisable to set up an automatic informative response or request to send a message to another e-mail address, but not to access e-mails in the mail box.

**Biometric personal data**
- A controller used a Face ID system as an attendance system, allowing to record the time of arrival and departure of individuals on the site based on facial recognition. The face scans were performed directly on a terminal located at the workplace. Scans were transformed by mathematical algorithms into a so-called hash, which remained to be stored in the terminal. The inspected controller processed both employees' identification and professional data as well as information about their attendance through the Face ID system. The Office pointed out that this case was very specific as the inspected person was able to demonstrate that the processing of biometric data is necessary for the fulfilment of the specific duties of the controller (in particular safety at large construction sites). The inspected entity was not able to achieve this compliance by other, less invasive means (as previously used less invasive methods proved to be ineffective). However, in this context, it is necessary to point out that under normal circumstances employers cannot process biometric data for these purposes.

- Another controller processed biometric personal data (voice biometry) to verify the identity of the client when calling the client. Processing was based on the consent of the data subjects. Consent to the provision of voice biometrics was voluntary and the data subjects could withdraw at any time on a toll-free telephone line. The Office did not find any breach in relation to this processing of personal data.

# C. Unsolicited commercial communications

**The Office recommended that entrepreneurs who obtain consent to send commercial communications via some website form (e.g. by filling in an e-mail address on company's websites) should send a request for confirmation to such e-mail address. As a rule, demonstrable consent is only given upon confirmation of this request from such e-mail address (for example by clicking on a link provided or sending a reply).**

The Office also recommended that messages containing commercial communication should be labelled as commercial messages already in the subject of the message, for example by explicitly referring to "commercial message", "newsletter" etc.

The Office stated that the identification of the entity whose products, goods or services are promoted by the commercial communication must be provided in a clear manner, i.e. including its business name and possibly other identifiers such as company's ID or its registered office, VAT number, business address etc. The Office further pointed out that this information must be contained in the commercial communication itself, it is thus not sufficient to include a link that would redirect the addressee to such information.

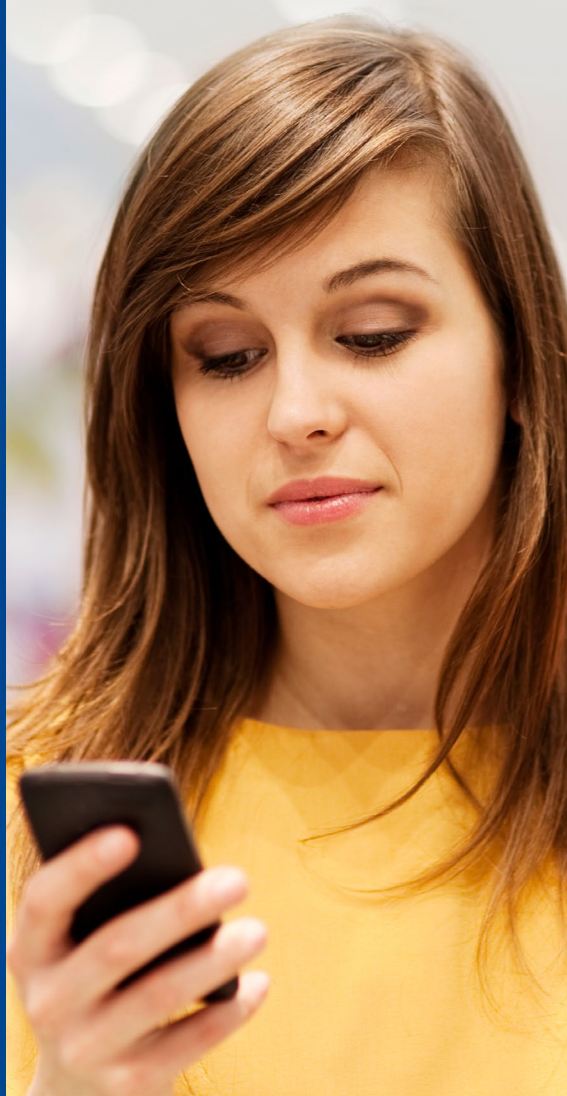
The Office also pointed out that all online commercial communications must contain a link to unsubscribe from the commercial communications.

# D. Reporting of personal data breaches

**Under GDPR, controllers are obligated to report personal data breaches to the Office unless the violation is unlikely to result in a risk to the rights and freedoms of data subjects. Since this obligation was introduced, the Office has received 600 notifications of personal data breaches.**

Many of them lead to unauthorised access to an information system through a successful phishing attack. Usually, the attackers obtained (and subsequently misused) the access credentials from the controller or processor's staff, on the basis of a misleading or fake e-mail sent to these employees. The cases mainly involved information theft but also the sending of other phishing e-mails to employees or contacts the mailbox user communicated with. A large proportion of the successful phishing attacks resulted in malicious software infecting an information system to encrypt data. Payment of ransom was demanded to decrypt the data. Regular backups of information provide an effective defence against this form of cybercrime (ransomware). In such a case, the necessary data can be recovered after the ransomware attack, while ensuring that the organization can continue its operations unhindered.

To enable reporting of personal data breaches, especially when controllers do not have a Data Protection Officer, a **form** is available on the Office's website. It contains all the necessary elements for assessing the severity of a breach.



# E. Second instance decisions of the Office published

**The Office has published selected anonymized second instance decisions of the Office Chairman on its website. The Chairman may revoke, amend or confirm the decisions of the Office. Its verdicts cannot be appealed but only challenged by an action filed to the respective administrative court.**

In 2019, the Chairman confirmed 7 out of 10 first instance decisions of the Office. In two cases, he changed the first instance decision so that the Office refrained from imposing a fine. This was because the Czech Act on Personal Data Processing had come into force, specifying that penalties may not be imposed on public bodies. In one case, the Chairman reduced the fine imposed because he considered the penalty disproportionate.

# F. Data Protection Impact Assessment methodology published for public discussion

**On its website, the Office published the Data Protection Impact Assessment (the "DPIA") methodology for public discussion. The DPIA must be carried out by every controller when the nature, scope, context or purposes of the processing are likely to result in a high risk to the rights and freedoms of natural persons.**

Previously published materials (on the Office's website **here** and **here**) on the obligation of controllers to carry out a DPIA describes in which cases it must or does not have to be made. The currently published methodology provides guidance on how to proceed in this matter, i.e. how to execute the DPIA when it has to be made. The methodology (in the version for public discussion) can be found on the Office's website (here).

# G. "Banking identity" could be used in the communication with the state

**Major Czech banks in cooperation with the public sector have come together to introduce an innovative solution that is supposed to enable the internet banking users to use the banking identity for communication with state authorities as well as with private companies.**

The major goal of the project SONIA is to provide the citizens (the banks´ clients), a possibility to arrange various matters in relation to the state authorities or private companies electronically. Currently the Czech Republic is lacking a widely spread digital proof of identity that could be used in the process of identity verification often required vis-à-vis the state authorities and private service providers.

Due to the fact that more than a half of the Czech population uses the internet banking services, using the banking identity within online identity verification process could bring the citizens, the service providers and the state lots of benefits. Particularly, project SONIA should open new possibilities in relation to the access to the e-government services. Further, it aims to make the e-government available to a broader scale of the citizens and it is also supposed to offer new ways of identification to the private service providers.

Necessary proposed legislative changes concern several acts, including the Bank Act, the AML Act, the Electronic Identification Act and the Act on Public Administration Information Systems. In practice, these legislative changes should provide the banks with a permission to provide the electronic banking identity, to create an entity that will create a link between the banks and the service providers, to access registries, and should overall enable the electronic identification from the AML perspective etc.

The respective legislative proposals are currently at the beginning of the legislative process and the optimistic outlooks suggest that it could be accepted in months to come.

# If you have any questions, please let us know


**Viktor Dušek**

Counsel
KPMG in the Czech Republic
+420222123746
vdusek@kpmg.cz

**Filip Horák**

Associate Manager
KPMG in the Czech Republic
+420222123169
fhorak@kpmg.cz

**Ladislav Karas**

Associate
KPMG in the Czech Republic
+420222123276
lkaras@kpmg.cz

**Ondřej Vykoukal**

Associate
KPMG in the Czech Republic
+420222123660
ovykoukal@kpmg.cz

# Germany

A. German Conference of Data Protection Authorities published new German GDPR fining guidelines

B. First German million euro fine issued by the Berlin DPA

# A. German Conference of Data Protection Authorities published new German GDPR fining guidelines

**On 14 October 2019 the German Conference of Data Protection Authorities (DSK) published their guidelines for calculating administrative fines under Article 83 GDPR. The new scoring model could make fines of tens of millions of euros a reality in Germany.**

**The guidelines provide a basis for the German data protection authorities (DPAs). By using the guidelines, fines for data protection infringements will be imposed according to a uniform procedure to secure a comprehensible, transparent and just approach of setting fines.**

## GDPR violations will be calculated in five steps:

1. Assign the undertaking based on the annual turnover
2. Determine the average annual turnover
3. Calculate the 'daily rate' by dividing the average annual turnover by 360
4. Multiply the base value by a factor reflecting the seriousness of the infringement
5. Adjust the value determined under step 4 based on aggravating and mitigating circumstances.

## Step 1:

**The undertakings are assigned to a group based on their total worldwide turnover** of **the preceding financial year. The undertaking can be categorized as**

- microenterprise: up to EUR 2 million annual turnover;
- small enterprise: EUR 2 million to EUR 10 million annual turnover;
- medium-sized enterprise: EUR 10 million to EUR 50 million annual turnover
- large-scale enterprise: more than EUR 50 million annual turnover.

Relevant for determining the undertaking's turnover is the 'functional undertaking' as understood under Articles 101 and 102 Treaty on the Functioning of the European Union (TFEU). The consequence is that parent companies and subsidiaries are regarded as an economic unit. Therefore, the total turnover of the group of companies will be used as the basis for calculating the fine.

## Step 2:

**This step is only relevant for undertakings with no more than EUR 500 million annual turnover. In such case the DPA apply a fixed 'average annual turnover fee'. For undertakings with more than EUR 500 million annual turnover further calculations will be based on the actual turnover.**

## Step 3:

**The DPAs determine the 'daily rate' by dividing the calculated average annual turnover of the undertaking for the preceding financial year by 360 days.**

## Step 4:

**The daily rate calculated using step 3 will be multiplied by a factor between 1 and 7.2 regarding infringements under Article 83 (4) GDPR or between 1 and 14.4 for infringements under Article 83 (5) and (6) GDPR. The factor depends on the severity of the infringement.**

**minor violation:**
- 1 to 2 (under Article 83 (4) GDPR) or
  1 to 4 (under Article 83 (5) and (6) GDPR)

**medium violation:**
- 2 to 4 (Article 83 (4) GDPR) or
  4 to 8 (Article 83 (5) and (6) GDPR)

**severe violation:**
- 4 to 6 (Article 83 (4) GDPR) or
  8 to 12 (Article 83 (5) and (6) GDPR)

**very severe violation:**
- 6 to 7.2 (Article 83 (4) GDPR) or
  12 to 14.4 (Article 83 (5) and (6) GDPR)

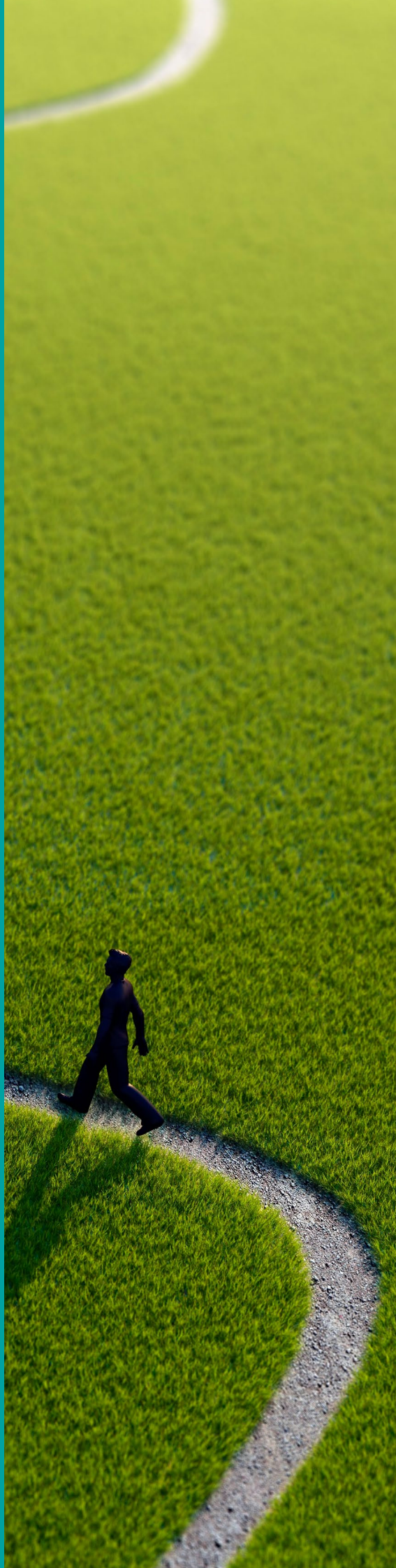
The outcome of this severity assessment represents the so-called 'regular fine corridor'. After receiving the 'regular fine corridor' the DPAs calculate the median value of this corridor. The further calculation of the fine is based on this value.

## Step 5:

**As a final step, the DPAs apply a percentage factor, considering any wider circumstances relevant to the infringement. The calculation below shows an example of how the percentage factors could look like.**

- degree of fault (-25% to +50%)
- mitigation measures taken by the controller or processor (-25% to +25%)
- degree of responsibility having regard to Article 25 and 32 (-25% to +50%)
- relevant previous infringements (0% to +300%)
- cooperation with the DPA (0% to +25%)
- manner in which the infringement became known to the DPA (-25% to +10%)
- compliance with measures ordered by the DPA (0% to +50%)
- adherence to approved codes of conduct or approved certification mechanisms (-25% to +10%)

The application of this model would lead to significantly higher GDPR fines than those imposed by German DPAs so far and serious penalty risks for undertakings with a high turnover.



# B. First German million euro fine issued by the Berlin DPA

**In September 2019, the Berlin Data Protection Authority (Berlin DPA) imposed an EUR 195,407 fine on a food delivery company. Only a month later a 14.5 million Euro fine was issued against a real estate company for violations of the GDPR. This marks a shift in German DPAs fining practice.**

First German six-digit fine: In September 2019, the Berlin DPA fined a food delivery company EUR 195,407 for the non-observance of the rights of data subjects under the GDPR. The company disregarded the right to information on the processing of data (Article 15 GDPR), the right to deletion (Article 17 GDPR) and the right to object (Article 21 GDPR). Former customers had complained that their data had not been deleted for years, even though they did not use the delivery service platform anymore. The Berlin DPA also announced that eight former customers received unwanted advertising emails – one of them even received 15 of those emails – despite an explicit objection. The company explained that some violations occurred because of technical errors or oversights caused by employees.

The Berlin DPA pointed out that a company that processes personal data must be technically and organizationally able to fulfil arising requests from data subjects without delay. Despite various instructions of the DPA sufficient measures had not been implemented by the company. To determine the amount of the fines, nature, gravity and duration of the infringement was taken into account as well as measures taken by the company to mitigate the consequences.

First German million euro fine: A few weeks after above-mentioned six-digit fine has been imposed, Berlin DPA fined a real estate company EUR 14.5 million. This company is reproached for storing their tenants' personal data without examining if this is lawful and necessary. According to the statement of the Berlin DPA Maja Smoltczyk the archiving system of the company does not allow the deletion of data. Therefore, information about the tenants' salary and account statements, self-disclosure, employment contracts, tax, social and health insurance data is stored for years. A so called 'data graveyard' could be highly vulnerable for cybercrime and involve high risks for data subjects, the DPA stated.

Two years earlier, the Berlin DPA had already informed the company about their insufficient archiving system, but no modifications have been made. Changes planed got stuck in preparation stage. The fine notice is not yet legally binding. The company already announced to lodge an objection.

By imposing the above-mentioned fines against both companies the Berlin DPA shifted the previous practice of German DPAs issuing much smaller fines. The fines imposed before ranged from a few hundred euros to five-digit amounts and therefore were much lower than fines imposed for example in France and UK.

The Berlin DPA disclosed that the highest possible fine against the real estate company would have been an amount of EUR 28 million. Because the company realized first measures of improvement and none of the data was misused the amount of the fine was reduced.

Due to this rigid approach of the Berlin DPA multi-million GDPR fines are now a reality in Germany.

# If you have any questions, please let us know

**Sebastian Hoegl, LL.M. (Wellington)**

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

**Maik Ringel**

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

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

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

**Thorsten Jansen**

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

# Italy

A. New rules per credit reporting system set out by Italian Privacy Authority

B. Investigation activities on food delivery, marketing, e-invoicing and banks by the Italian Garante Privacy

C. The Italian Privacy Authority contests the Italian 2020 tax decree with regard to e-invoicing

# A. New rules per credit reporting system set out by Italian Privacy Authority

**The Italian Privacy Authority (Garante Privacy) approved, after a complex review, the new "Code of conduct for credit reporting systems operated by private entities regarding consumer credit, creditworthiness and punctuality in payments" providing new rules for credit risk analysis**

Some of the innovations laid down in the new "Code" refer to greater safeguards for consumers registered in credit databases, transparency on the functioning of algorithms that analyse financial risk, openness to new technologies and fintech services, increasing the security measures taken to protect the data from unlawful access and to ensure reliability of the systems. The new "Code" was proposed by the trade associations and approved by Garante Privacy on 19th September 2019 after the review of the old Code of Ethics, nowadays obsolete due to the changes introduced by the European and national privacy legislation.

These new rules on credit risk analysis concern data on loans and mortgages, long-term rental and the most innovative forms of loan between private entities (the so called "peer-to-peer lending") managed through fintech platforms.

Due to the difficulty to collect data subjects' consent for the credit companies, in order to facilitate the proper functioning of the financial and credit market, the records may be processed on the basis of the legitimate interest of the companies participating in the credit reporting systems, as established by article 6, par. 1 let. f) of EU Regulation no. 679/2016 (GDPR). Only the relevant and necessary data for the credit risk assessment purposes may be processed, by providing complete information to data subject under art. 13 of the GDPR. For example, if the data subject apply for a mortgage and his application is rejected, the data subject will be able to know if the decision was taken also on the basis of the risk scoring given by an algorithm and, if so, to request to know the underlying logic.

In addition, the analytical and statistical models as well as the algorithms used in this process should be reviewed and updated at least every two years.

Some of the main novelties are listed below:
- Disclosure: more complete information about the data processed by the participating companies;
- Monitoring body: an independent body must be established to oversee the work of credit reporting systems;
- New forms of contact: instant messaging systems used on smartphones, in order to simplify the arrangements for informing data subjects prior to their registration in a credit reporting system or 'alert notices' may also be sent by means of instant messaging systems that ensure traceability of the delivery;
- New credit categories: the scope of registered data was extended to include various forms of leasing, hire, lending between private parties (peer to peer lending);
- Longer positive data retention: positive historical data on clients may be stored for 60 months to protect credit and to meet the legal obligations and the demand coming from supervisory bodies;
- Transparency in decisions: in the event of a denial of credit based on automated analysis, the data subject may request to know the logic underlying operation of algorithms;
- Pseudonymised data for the training of algorithms: algorithms may be 'trained' with pseudonymised data, i.e. data that can no longer be related to a specific entity;
- Security: additional measures are envisaged to protect data security and against unlawful access.

Nevertheless in the approval decision, the Garante Privacy requested some changes to the functioning of the monitoring body established by the Code in order to strengthen its independence and autonomy.

The new Code will become fully effective only upon completion of the accreditation procedure of the monitoring body which requires the favourable opinion of the EDPB (European Data Protection Board).

# B. Investigation activities on food delivery, marketing, e-invoicing and banks by the Italian Authority

## The inspection activities of the Italian Authority ("Garante Privacy") scheduled for the second half of 2019 have started

The inspections, more or less one hundred – carried out with the aid of Special Unit of the financial police ("Guardia di Finanza") – affects the processing of data carried out by banks, with particular regard to flows to the bank registry accounts, data processing performed by companies operating in the food delivery sector and those carried out by marketing companies.

The Garante Privacy focuses its attention also on other particular sectors such as:
- the databases of considerable size of the public entities;
- the flow of data processed in the management of reports of illegal conduct (so called, "whistleblowing");
- the profiling activities of loyalty card holders;
- the data processing activities performed by intermediaries offering electronic invoicing services;
- processing activities of private companies in the health sector.

The inspection activities will also focus on compliance with the rules on the disclosure of the information to data subject, on consent and on data retention. In addition to the inspections already scheduled for the second half of the year, the Italian Authority will be able to order further official inspections following reports or complaints of data subjects.

In the first six months of 2019, 65 inspections have been carried out, also with aid of Financial Police, focusing on call centers, marketing companies, important hotels, database of significant size of the public administration.

In the same period the revenues deriving from the sanctioning activities amounted to 1.222.955 euros while 86 ordinances have been adopted – some relating to complex cases involving multiple violations – for a total of 3,250,390 euros.

# C. The Italian Privacy Authority contests the Italian 2020 tax decree with regard to e-invoicing

**The Italian Privacy Authority (Garante Privacy) had already criticized the Italian regulation on electronic invoicing, firstly in November 2018 and lastly with the provision of 20 December 2018, considering this particular processing activity carried out by Italian Tax Authority and intermediary companies not compliant with privacy law.**

With a memorandum filed on November 5 at the Finance Committee of the Chamber, the Italian Privacy Authority (Garante Privacy) censored some aspects of the draft C.2220, converting the law decree no. 124 of October 26 2019, commonly known as the "2020 tax decree" (Decree).

In the opinion set out by Garante Privacy President Antonello Soro, the storage of data on files in .xml format, in the way established by the Decree, would be completely unnecessary having regard to the purposes pursued by the Italian Tax Authority. In particular Garante Privacy contested the integral storage of e-invoices where the provision of art.14 of the Decree "would, in fact, render the law illegitimate due to the contrast with the proportionality principle set out for the processing of personal data, as already established by the European Court of Justice as an essential hermeneutical parameter in this particular matter".

The storage of personal data for 8 years provided for by the Decree regards the integral documents of every information entered in the issuing phase, ie. each e-invoice issued or received by the Tax Authority would be stored "including non-tax-relevant data (also the recipients of the invoiced services) and those relating to the description of the services provided, for the purpose of carrying out timely investigations in the context of tax assessments, carried out also by the Italian Financial Police (Guardia di Finanza) ".

This form of retention therefore appears unjustified under the EU Regulation no. 679/2016 (GDPR), because of the huge amount of personal data that is not functional to the purpose pursued by the Tax Authority that – due to centralized filing of all the e-invoices- could lend itself to improper or illegitimate uses, could increase the risk of cyber attacks and, consequently, of data breaches as established by art. 33 GDPR.

Garante Privacy also claims that "we only have to use the data that are necessary to the specific processing purposes, we are not against electronic invoicing, but it is disproportionate to collect data unnecessary for tax purposes. It is useless, wrong and disproportionate because it costs a lot, there is a risk of hacking and certain data are not even useful for the Financial Police or the Tax Authority".

The memorandum filed by Garante Privacy asks for repentance when converting the Decree into law. President Antonello Soro said: "In particular, it will be auspicable to acquire, from the government, elements for overcoming the critical points already represented in the aforementioned provisions of the Garante, evaluating whether the memorization of such a large number of personal data is really functional for the related processing purposes and not replaceable with equally effective but less invasive measures or even only with the erasure of irrelevant – (unnecessary) – data that may be included in the e-invoices."

Therefore the Garante Privacy is willing to increase the security in the e-invoicing processing activities, by means of:
- stronger measures;
- compliance with general principles of GDPR;
- definition of roles and liabilities for all the processors in this specific processing activity (i.e. the Italian Tax Authority and all the intermediary companies);
- carrying out of data protection impact assessment.

It must be underlined that, although the opinion of the Garante Privacy is not binding for the government, it must still be taken into account with great attention, due to the prominent relevance of privacy matters nowadays.

# If you have any questions, please let us know


**Dr. Michele Giordano**

Managing Partner
KPMG Studio Associato
KPMG in Italy
+393486561052
michelegiordano@kpmg.it

**Atty. Paola Casaccino**

Attorney-at-law
Senior Manager Governance
Risk & Compliance Services
KPMG in Italy
+393484420380
pcasaccino@kpmg.it

**Atty. Alessandro Legnante**

Attorney-at-law
Senior Legal Specialist
Risk & Compliance Services
KPMG in Italy
+393455989855
alegnante@kpmg.it

# Spain

A. Guidance by the Spanish Data Protection Authority on “Privacy by Design”

B. Guidance by the Spanish Data Protection Authority on “the use of cookies”

C. Agreement between the Spanish National Institute for Statistics (INE) and telecom companies on the use of mobility data

# A. Guidance by the Spanish Data Protection Authority on "Privacy by Design"

**The Spanish Data Protection Authority (AEPD) has published a piece of Guidance on "Privacy by Design" with the aim of providing standards that facilitate the incorporation of data protection principles and privacy requirements into new products or services from the moment that they begin to be designed.**

In a context where organizations are constantly developing products and services based on an intensive use of personal data and disruptive technologies and where, as a consequence of this, inherence in the privacy of the citizens is extremely high, in addition to effective and efficient technical and organizational measures aiming at protecting said information, it is necessary that these organizations adopt a privacy by design approach as the only way to ensure that said inherence on the privacy of citizens is as limited as possible.

Both data controllers and data processors must adopt this approach as part of their duty of care when designing and/or selecting products, services, providers, etc. To support controllers and processors in this task, the AEPD has provided a piece of guidance clarifying that privacy must be an integral part of the nature of products or services and a driver for their design from the earliest stages of their development.

The piece of guidance approved summarizes the phases for implementing privacy by design as follows:

**Phase 1:**
- Conducting a risk analysis of the data processing to define the specific objectives of data protection (unlinkability, transparency and intervenability) as well as security goals (confidentiality, availability and integrity)

**Phase 2:**
- Studying the privacy design strategies that will allow specification of the requirements to be fulfilled in order to achieve each privacy goal. These strategies could be divided into two categories: data oriented ('minimise', 'hide', 'separate', 'abstract') and process oriented ('inform', 'control', 'enforce' and 'demonstrate).

**Phase 3:**
- The selected strategies shall be integrated by means of available solutions, that is to say, privacy design patterns that deal with common and reiterated problems.

**Phase 4:**
- Implementing these patterns in the development stage. Implementation shall be carried out by developer teams either by programming the code with the necessary functionality or whenever possible, by using existing ICT solutions, i.e., Privacy Enhancing Technologies (PETS).

# B. Guidance by the Spanish Data Protection Authority on "the use of cookies"

**The Spanish Data Protection Authority (AEPD) has published a new piece of "Guidance on the use of Cookies", replacing the previous piece (dated 2013) and adapting its content to the GDPR, in particular with regard to the conditions for properly obtaining the informed consent of the user for the installation of cookies.**

The new "Guidance on the use of the Cookies" published by the AEPD, in collaboration with the industry (ADIGITAL, advertisers, AUTOCONTROL and IAB Spain), interprets, in the light of the requirements laid down by the GDPR, the information society providers' duties to inform and obtain the consent of the users for the installation of cookies on their devices, as set forth by the Spanish information society service and e-commerce regulation (the Spanish regulation implementing into the Spanish legal system the obligations set forth by the Directive 2002/58/EC on privacy and electronic communications, as amended by the Directive 2009/136/EC).

The AEPD indicates, stepping out of the line set out by the EUCJ in its recent judgment of 1 October 2019 [Case C-673/17 (Planet49)], that it is not necessary to inform (neither to collect the consent of the user) for the installation of technical/session cookies. The minimum information to be provided on the rest of cookies comprises: (i) their definition and generic functions; (ii) information regarding the type of cookies and their purpose; (iii) information regarding of the party that use them; (iv) information about the way to accept, reject, revoke the consent or delete them; (v) information about any international transfer to recipients located in third countries (if applicable); information about the logic used, its importance and consequence foreseen for the user when a profiling of the users that may produce legal effects or significantly affect them is carried out; and (v) their storage period. Regarding the way to provide this information, the AEPD suggests that information should be provided in two layers. Should this system be used, the information to be provided in the first layer must include the identity of the information society provider, the purpose of the cookies and if they are self-owned or third party cookies, generic information about the type of data that will be collected and a link to the web page by means of which extended information is provided in a second layer. The information in the first layer must be completed with a system or user configuration panel allowing to choose between accepting or rejecting all cookies in a granular form, or a link that leads to that system or panel. With respect to the degree of granularity, cookies should be grouped by purpose, avoiding the maximum degree of granularity (cookie to cookie selection).

**Spain**

In relation to the obligation of obtaining consent for the installation of cookies, the AEPD allows for the possibility of obtaining the consent of the users by means of low intensity positive actions (such as scrolling down or selecting specific content within the web page), except in cases in which special categories of data are collected, and provided that the cookies notice (banner) is inserted in a clearly visible/prominent place and that, due to its characteristics, said notice cannot go unnoticed by the user. In this case, however, a button allowing for the rejection of all cookies must be integrated in the first layer notice. This consent collection scheme does neither seem to be fully aligned with the pronouncements made by the ECJ in its judgment in Case C-673/17 (Planet49).

Finally and among other matters, the guide also provides a maximum indicative period for updating the consent or rejection of cookies, which must not exceed 24 months, and allows for a total or partial denial of a service if the installation of cookies is not accepted, except in those cases in which said denial could prevent the exercise of a legally recognised right of the user. A position that might be deemed to be incompatible in some cases with the fact that the consent is granted in a truly free manner, as required under the GDPR.

# C. Agreement between the Spanish National Institute for Statistics (INE) and telecom companies on the use of mobility data

**The Spanish Statistical Office (INE) is focusing on technology and big data to carry out its studies. In line with this, it has launched a project that requires analysing the location of a limited number of Spanish mobile phones for eight days in order to compile statistics on the regular movements of citizens and to determine where the public services and infrastructures need to be strengthen. This will enable to detect patterns that can be used by local councils to make decisions regarding transport and mobility.**

The project will be carried out through an agreement with the three main Spanish telecommunications operators, which will provide INE with data consisting of the number of terminals in a given area at diffent times. INE, through an institutional statement, has clarified that the data to be processed within the framework of the project will be completely anonymous, and it will only receive a count of terminals in the form of aggregated tables of results, but not the data relating to the phone line holders, so that in no case will the INE be able to track the position of any terminal.

INE's position is that, to the extent that the data transferred to INE consist in anonymised data (i.e. INE cannot identify any user), the data protection principles would not apply. However, on the basis that anonymization for statistical purposes is a data processing activity itself, data controllers (i.e. the telecommunications operators) should collect and process these data in accordance with the GDPR and Constitutional Act 3/2018, of 5 December 2018, on the protection of personal data and guarantee of the digital rights (hereinafter, "LOPDGDD", in its Spanish acronym) and, consequently, should previously inform the data subjects about this processing activity. In relation to the legal basis of the processing, there is some controversy on whether telecommunications operators can rely on a legitimate interest or the processing requires collecting the consent of the affected data subjects. There are some voices that even defend that these data cannot be used by the telecommunication operators for this purpose, as collection of the same is only licit for certain purposes set out in the telecommunication applicable regulations.

## Spain

Although the Spanish Data Protection Authoriy has admitted that massive data processing activities can be carried out using technologies such as Big Data or Artificial Intelligence provided that a series of privacy protection processes and guarantees have been applied, it has announced that it is studying the case and that has requested INE to provide some information on the protocols it has established with the telecommunications operators in order to receive these data. No further information about the outcome of this investigation carried out by the AEPD has been made public to date.

# If you have any questions, please let us know


**Eric Romero**

Senior Manager
KPMG in Spain
+34932532900
ericromero@kpmg.es

**Claire Murphy**

Lawyer
KPMG in Spain
+34914563400
clairemurphy3@kpmg.es

# Russia

## A. Up to EUR 260,000 fines may be established for violation of the localization requirement in Russia

# A. Up to EUR 260,000 fines may be established for violation of the localization requirement in Russia

**The State Duma of the Russian Federation (the legislative branch) is considering a draft law that imposes significant fines for violation of the localization requirement**

What is localization requirement? Since 2015, when collecting personal data, a personal data operator must make sure that the personal data of Russian citizens are recorded, classified, accumulated, stored, updated/amended, and extracted using databases located in Russia.

What is the practical impact of the localization? According to explanations of the Ministry of Telecom and Mass Communications of the Russian Federation, the localization requirement implies that the principal personal data database (relating to Russian citizens) must be stored in Russia. In other words, all personal data must initially be located in Russia (e.g. transferred to the data center located in Russia). A copy of this database may subsequently be transferred abroad (i.e. outside Russia). Furthermore, the database located in Russia must not contain a smaller amount of personal data compared to the personal data stored in the database located abroad.

What is the liability for violation of the localization requirement? The current Russian legislation does not contain any special sanctions for failure to comply with the localization requirement (except for insignificant general fines). However, the State Duma is considering a draft law that introduces amendments to the Administrative Offences Code of the Russian Federation. According to the proposed amendments, a fine of approx. EUR 3,000 to 7,100 will be established for officials breaching the localization requirement (in case of repeated violations, the fine will amount to approx. EUR 7,100 to 14,200) and of approx. EUR 28,500 to 85,300 for legal entities (in case of repeated violations, the fine will amount to approx. EUR 85,300 to 260,000).

We assess the possibility of adopting the law establishing fines (not necessarily in this specific version) for violation of the localization requirement as high. We will keep you informed of the progress of adoption of this law and recommend to all clients to bring the processing of personal data of Russian citizens into compliance with the Russian legislation preventively.

# If you have any questions, please let us know


**Ekaterina Tsybikova**

Director
KPMG in Russia
+78123137300 (ext.13672)
ETsybikova@kpmg.ru

**Anton Fedotov**

Senior Lawyer
KPMG in Russia
+78123137300 (ext.37326)
antonfedotov@kpmg.ru

**Grigoriy Moskalev**

Senior Legal Consultant
KPMG in Russia
+78123137300 (ext.36099)
gmoskalev@kpmg.ru