KPMG

# Data privacy newsletter

**KPMG Global Legal Services**

July/August 2019

# Contents

# Introduction

**Welcome to the second 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 GDPR completed its first year in force, we bring to your attention fresh experience from various jurisdictions. Belgium reports that its Data Protection Authority is 'fully operational' while in Poland 170 particular acts have been updated with regard to the GDPR, especially the Labour code. In Germany, considerable discussions were initiated regarding the trial tactics and the right to information according to the GDPR.

In further developments, the UK Data Protection Authority has announced its intention to levy its first major fines under the GDPR. A significant fine has already been issued by the Hellenic Data Protection Authority in Greece. The Italian authorities are not far behind Greece, and imposed a 1 million Euro fine on Facebook.

Internet users are not safe either when using popular mobile apps attracting millions of mainly younger people. Authorities in Poland have sounded a note of caution, issuing a warning to app users.

As data protection lawyers we aim to reduce risks for our clients. Many of these are hidden in cyberspace. What if the National Revenue Agency suffers a hacker attack? Learn from the case in Bulgaria where a leak of confidential information affected over 4 million citizens, as well as commercial companies. You can also find out about the outlines of the Law on Cybersecurity in Vietnam which seeks to regulate some activities in cyberspace.

There is much more to read in our compilation of developments in the area of data privacy, especially as many of them can have cross-border impacts.

# International

## International Standard for Privacy Information Management Systems Are Published

The ISO (the International Organization for Standardization which forms a specialized system for worldwide standardization) has published the first International Standard for Privacy Information Management. ISO/IEC 27701 specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are personal data controllers and/or processors.

## European Data Protection Board Adopts Guidelines on Video Surveillance

The Twelfth Plenary session of the European Data Protection Board took place on 9th and 10th July. At this session, the board adopted guidelines on the processing of personal data through video devices, which clarify how the GDPR applies to the processing of personal data when using video devices and aim to ensure the consistent application of the GDPR in this regard.

The new Guidelines describe in detail the requirements imposed by the GDPR for the processing of personal data within the framework of video surveillance technologies. The document presents a number of practical situations with examples of facial recognition, targeted advertising, traffic (dash cams), and crime prevention.

## The CJEU Decision in the Fashion ID Case Regarding Facebook's "Like" Button

The Court of Justice of the European Union ("CJEU") has issued its judgment in the Fashion ID Case. This decision deals with the assessment of who has the responsibility for complying with data protection regulations when embedding third-party features on websites. The CJEU decided that the website operator featuring the Facebook "Like" button can qualify as a controller, jointly with Facebook, and is therefore directly responsible for complying with all legal obligations in this respect.

The CJEU specified that the website operator is considered as the controller only with respect to the collection of the data (which, however, entails the obligation to inform users that their personal data will be transferred to Facebook) and its transfer to Facebook. It will not be considered a controller in respect of any subsequent personal data processing carried out by Facebook as this cannot be affected by the website operator.

This decision can affect also other third-party technologies which are incorporated into websites, such as cookies.

# Belgium

A. Status of the Belgian DPA

B. One year of GDPR in Belgium

# Status of the Belgian DPA

**The Belgian Data Protection Authority ("DPA"), which is the successor of the Belgian Privacy Commission as of 25 May 2018, is fully operational as of the first quarter of 2019, when the appointment of the members of the Belgian DPA was finalized.**

Its chairman and director of General Affairs recently stated that all necessary actions are now being taken to ensure proper GDPR enforcement in Belgium.

## Structure

**The body of the Belgian DPA ("Gegevensbeschermingsautoriteit"/ "Autorité de protection des données") is structured into the following six divisions:**

a) Executive Board
b) General Affairs
c) Front Office
d) Knowledge Centre
e) Inspection Service
f) Litigation Chamber

The DPA members residing in their respective divisions are appointed for six years by the Belgian Federal House of Representatives. The six-year term can only be renewed once. Each division has its specific competences and tasks (as set out in detail in national Belgian law).

## First Fines

**The Litigation Chamber (i.e. the administrative disputes body) has also published its first two decisions in the meanwhile:**

- An administrative fine of EUR 2,000.00 was issued for the unauthorized use of personal data by the mayor of a city for campaign purposes during municipal elections in 2018. The DPA established a breach of the purpose limitation principle as embedded in the GDPR.
- A reprimand to the FPS Public Health was given for its failure to respond to a request under the right of access. Short term actions were imposed to ensure GDPR compliance.

## SME Campaign

Furthermore, the Belgian DPA has recently launched a campaign to raise GDPR awareness for small and medium sized enterprises (SMEs). Different actions have been planned, e.g. the drafting of a code of conduct and the set-up of a collective communication platform. Furthermore, the DPA has sent out enquiry requests to professional bodies representing SMEs and to professional networks of data protection officers.

The campaign goal is to better assist and support SMEs in applying the privacy legislation.

# One year of GDPR in Belgium

**The Belgian DPA has issued its annual report of 2018: "GDPR in numbers". Overall, there was a strong increase in the number of requests (i.e. Q & A, mediation, investigation, etc.), data breach reports and general case work.**

## Regulatory

- The Belgian DPA was formally founded by the Law of 3 December 2017.
- The GDPR has been transposed into the Belgian national framework by the Law of 31 July 2018 for the protection of natural persons regarding the processing of personal data.

## Data Protection Officers

- As of 25 May 2018, over 3,666 DPOs have been appointed in Belgium.
- Data Breaches
- 445 data breaches were reported in 2018. The most vulnerable sectors are those concerned with financial activities and insurance, healthcare, public administration and defence.

## Investigation Records

- The Inspection Service of the Belgian DPA has investigated 70 cases. The most common issues involved data subject rights, direct marketing, and CCTV.

## Belgian DPA

- The DPA's Knowledge Centre issued advice over 215 times in 2018 on the processing of personal data.
- An amount of 7,182 "working files" were processed, which includes: 6,224 information requests, 295 demands for mediation, 218 audit files, and 445 data breach reports.
- The DPA's operational budget for 2018 was EUR 8,217,300.

# If you have any questions, please let us know

**Tim Fransen**

Senior Counsel
K law Belgium
+32 (0)38211809
timfransen@klaw.be

**Matthias Bruynseraede**

Junior Associate
K law Belgium
+32 (0)38211977
mbruynseraede@klaw.be

# Bulgaria

A. Data retention in the recruitment process

B. Controllership over data in clinical trials

C. How to excercise data subject rights by a proxy?

D. National Revenue Agency suffers a hacker attack

# Data retention in the recruitment process

**Personal data originating from CVs and other documents and then included in recruitment related documents drafted by the employer may be retained for up to 3 years.**

The Bulgarian Commission for Personal Data Protection ("CPDP") issued a new statement concerning data retention practices in the recruitment process. The statement aims to reconcile the presumable conflict between the Personal Data Protection Act and the Protection Against Discrimination Act, both of which govern data retention in the recruitment process.

The CPDP opined that source documents of job applicants such as CVs, diplomas, cover letters, etc. must be stored for not longer than 6 months, unless the applicant agreed to a longer term, as specifically prescribed in the Personal Data Protection Act. Furthermore, any original or notarized copies of diplomas, certificates or other testimonial documents requested by the employer shall be returned to the job applicant within 6 months of the campaign closure.

According to CPDP's statement, however, pieces of personal data **originating from the source documents** and then **included in recruitment related documents** drafted by the employer may be retained. This is allowed in order to secure evidence in case anti-discrimination procedures are initiated within the 3-year term provided in the anti-discriminatory legislation. Employers should in any case comply with data minimization and storage limitation principles.

# Controllership over data in clinical trials

**Medical institutions and the sponsor of a clinical trial are joint data controllers when processing personal data of trial participants.**

The Bulgarian Commission for Personal Data Protection ("CPDP") issued a new opinion concerning the controllership over personal data and the roles of the stakeholders in the course of clinical trials.

This is the first time the CPDP provides an opinion on the relationship between the sponsor and the medical institution in the context of clinical trials. Despite being subject to various analyses and publications, currently there is no consistent practice on this matter across the EU countries.

The CPDP draws the final conclusion that within clinical trials medical institutions and the sponsor process personal data of trial participants both acting as data controllers. Based on the facts of the particular case, the relationship between the sponsor and the hospital is deemed to constitute co-controllership over the trial participants' personal data.

The matter was referred to the CPDP by a pharmaceutical company acting as the sponsor of clinical trials. (The sponsor is the principal stakeholder in a clinical trial and is responsible for initiating the clinical trial, its management and for securing financing as well.)

The CPDP further states that onsite processing activities within a clinical trial cannot be carried out on behalf of the sponsor. This is because only a medical institution is allowed to do so by law. Therefore, the relationship between sponsor and hospital cannot be governed by a Data Processing Agreement under Art. 28 of the GDPR.

The CPDP also makes a reference to the analysis on the controllership over clinical trial participants' data, presented by the former WP 29 (now the European Data Protection Board). While analyzing the concepts of controller and processor, the WP 29 illustrates by example that the sponsor and medical institutions are joint controllers in terms of personal data processing.

Thus, the sponsor and the medical institutions must comply with the rules for joint controllership set forth in the GDPR, i.e. they must outline their responsibilities contractually, if the latter have not been explicitly arranged by an EU or local law, in a transparent manner. The parties must ensure it is easy for the trial participants to exercise their rights as data subject's requests, including by defining each party's role in making relevant disclosures of privacy information as set forth in the GDPR, as well as any other relevant matter, e.g. the appointing of a contact person for the trial.

Regardless of any covenant, however, trial participants are allowed to exercise their rights against any of the joint controllers.

# How to excercise data subject rights by a proxy?

**No notarized power of attorney is necessary to exercise data subject rights on someone else's behalf as his/her proxy.**

The Commission for Personal Data Protection ("CPDP") was asked to provide its opinion on the right way to authorize a proxy to exercise data subject rights in the context of a patient-hospital relationship. The inquiring hospital could not determine if it should decline all data subject's requests made on behalf of a data subject, should the proxy not have a notarized power of attorney as evidence of his/her authority.

Considering the provisions of the Personal Data Protection Act (PDPA) and the absence of a specific requirement provided by the health laws for the form of the power of attorney, the CPDP ruled that in the case of exercising the right of access, erasure, rectification or any other data subject's right by a proxy, the controller is not entitled to request the production of a notary certified power of attorney.

By reference to contract law, the CPDP also stated that since the PDPA requires a data subject's request to be in writing, then the power of attorney, executed in a simple written form, shall be considered valid evidence of authorization in favor of the proxy.

Although the CPDP's statement concerned hospitals in particular, the conclusions of the commission are of a principle nature and their arguments and statements are expected to have widespread effects and applicability.

# National Revenue Agency suffers a hacker attack

**The National Revenue Agency suffered a data breach affecting over 4 million living Bulgarian and foreign citizens' personal data.**

On 15 July 2019 the National Revenue Agency ("NRA") established that nearly 3% of its database was compromised through an unauthorized access by a hacker to its system affecting over 4 million living Bulgarian and foreign citizens, as well as confidential information about commercial companies.

The information apparently related to the database of the NRA and other public authorities (registers of personal status, the social security institute, etc.) included names, personal identification numbers, addresses, tax returns, social and health insurance data (not medical condition data), payment details, social benefits, employment information, ID card details, etc.

On 17 July the NRA officially notified the The Commission for Personal Data Protection ("CPDP") of the breach to comply with its obligations set in the General Data Protection Regulation. The CPDP announced that the investigation of the breach will be completed by 20 August 2019.

Besides the notifications to the CPDP and to the affected individuals, published on its website, the NRA also notified the law enforcement authorities and the prosecution office.

The NRA deployed an online application for citizens to check whether their personal data was compromised. The system allows a reference by personal identification number (PIN) and a telephone number. Subsequently, the application was enhanced to allow access only with personal code issued by the NRA or a qualified electronic signature. A simple yes/no confirmation is sent back to a mobile number specified by the respective user of the application to exclude potential misuse of the platform.

The NRA announced that it had established that the leaked data for 189 individuals constituted a combination of names, PIN, address and ID card details. This group of affected individuals will be personally contacted by the agency.

Other measures applied by the NRA included the upload of answers and explanations to frequently asked questions related to the breach on the NRA's website. The NRA also undertook to block potentially unsecure online services and also commissioned a security audit to an external service provider.

Upon completion of the investigation over the matter, the CPDP prescribed mandatory corrective measures for the NRA in the aim of aligning the security level of the NRA's systems with the requirements of the applicable legislation.

On 29 August it was announced by the CPDP that the NRA is to suffer a pecuniary sanction for non-compliance with the rules of the GDPR to the amount of BGN 5.1 million. The CPDP takes into account the severity of the breach and the measures undertaken by the NRA to limit the negative effects of the breach.

The decree of the CPDP for imposing the sanction will be appealed before the court by the NRA.

# 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

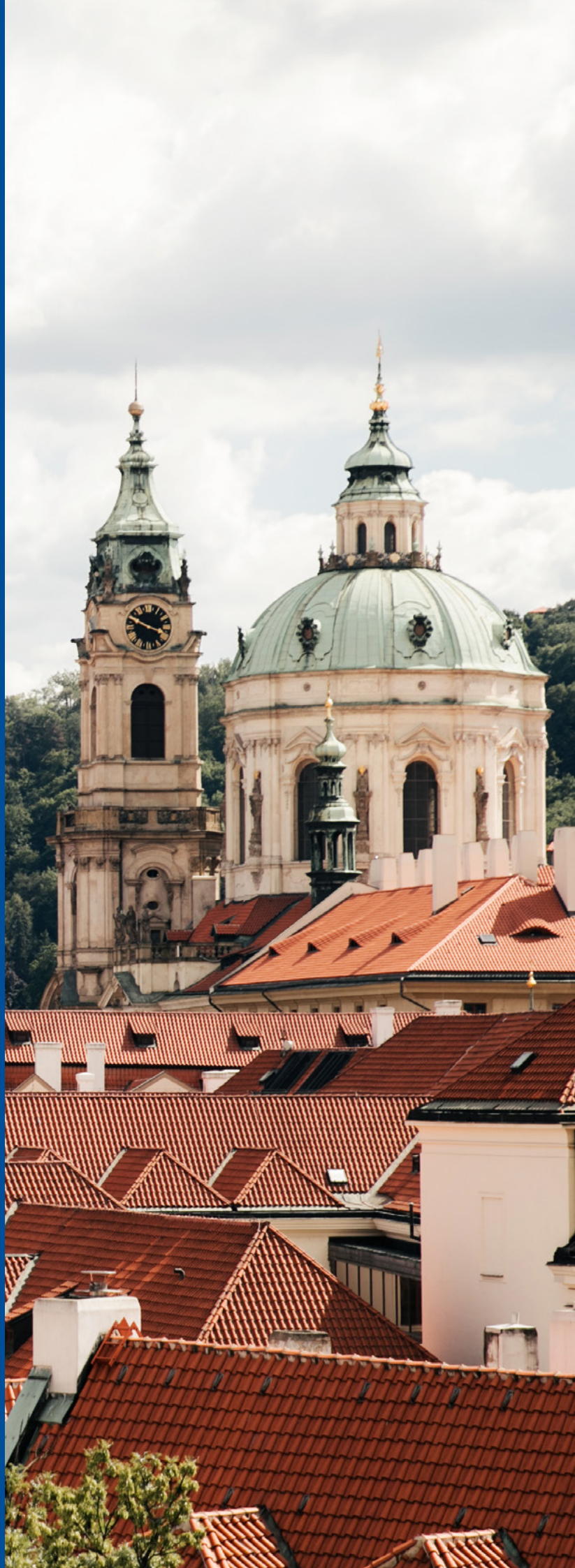
A. Proposal to amend the Labour Code with respect to processing of biometric data

B. Incapacity to impose administrative sanctions on public authorities

C. Czech translation of Guidelines on the processing of personal data through video devices

D. Admissibility of CCTV in prison cells

E. Draft Act on Whistle-blowers' Protection



# Proposal to amend the Labour Code with respect to processing of biometric data

**The Personal Data Protection Office ("Office") proposed to the Ministry of Labour and Social Affairs of the Czech Republic amendments to the Czech Labour Code with respect to the processing of employees' biometric data.**

The reason is that employers in the Czech Republic are increasingly using technologies based on biometric authentication, e.g. attendance systems based on fingerprints. According to the Office, it is necessary that the labour law takes into account the spread of biometric technologies in society and formulates basic requirements of personal data protection. Such statutory provision is needed according to the Office, especially with respect to Art. 9 of the GDPR that allows the processing of sensitive personal data only in very limited cases.

The proposed legislation aims to set forth that biometric data can be used for security reasons (control of access to production and other devices of the employer and access to the employer's premises) but it cannot be used e.g. to monitor attendance of the employees.

The matter of biometric data processing is widely discussed in the Czech Republic also with respect to some other cases. Generally, according to the Office statements, the processing of biometric data is being overused in the Czech Republic. For example, it recently criticized the use of such data for identifying and preventing unwanted persons from entering football stadiums.

# Incapacity to impose administrative sanctions on public authorities

For the first time, the Personal Data Protection Office ("Office") applied a new provision of the Czech Personal Data Processing Act, according to which no administrative sanction can be imposed on a public authority or a public entity. This exception is based on Art. 83 (7) of the GDPR which allows Member States to lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies.

Based on the Personal Data Processing Act, the Office has lost the power to impose any fines on public authorities and public entities, such as ministries, various administrative authorities or municipalities for offenses related to the protection of personal data. However, it may still continue to impose remedial measures on the public authorities and bodies.

# Czech translation of guidelines on the processing of personal data through video devices

**The Personal Data Protection Office ("Office") publishes a Czech translation of the European Data Protection Board's Guidelines on the processing of personal data through video devices (No. 3/2019) which were adopted by the EDPB in July in a version for public consultation. The guidelines aim to ensure consistent application of the GDPR in this regard.**

As part of the public consultation, both the general public and the professional public, citizens, associations or other entities may send their opinions and comments to the EDPB, which will be assessed and possibly incorporated. The Office encourages the public to participate in the public consultation, and emphasizes that it is the right of all interested parties, persons affected by video recording, as well as controllers, processors and technology suppliers to comment and point out practical and interpretative uncertainties in order to improve the guidelines.

# Admissibility of CCTV in prison cells

For the first time, the Personal Data Protection Office ("Office") applied a new provision of the Czech Personal Data Processing Act, according to which no administrative sanction can be imposed on a public authority or a public entity. This exception is based on Art. 83 (7) of the GDPR which allows Member States to lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies.

Based on the Personal Data Processing Act, the Office has lost the power to impose any fines on public authorities and public entities, such as ministries, various administrative authorities or municipalities for offenses related to the protection of personal data. However, it may still continue to impose remedial measures on the public authorities and bodies.

# Draft Act on Whistle-blowers' Protection

**Privacy matters are tightly connected to the protection of whistle-blowers and the possibility to remain anonymous in certain cases. In this respect, within the legislation process a draft Act on Whistle-blowers' Protection is currently being prepared.**

This act should regulate conditions for filing notifications to authorities, providing protection to persons who have made a notification, and establishing a new Whistle-Blowers' Protection Agency.

Employers (i) who employ more than 50 employees; (ii) with a total annual turnover or an annual balance sheet exceeding EUR 10 million; (iii) who are the obliged entity under the AML act; (iv) and the public contracting authority pursuant to the Public Procurement Act will have to introduce an internal notification system. The internal notification system should lay down rules for the submission of notifications, allowing them to be made orally, in paper form or electronically, and even anonymously.

This bill is subject to criticism, especially because the act was prepared before the adoption of the respective EU directive. It may therefore happen that the Czech act will be at variance with the directive, instead of deriving from it. Thus, it is not known, whether the bill will be passed.

# If you have any questions, please let us know


**Viktor Dušek**

Counsel
KPMG in the Czech Republic
+420 222 123 746
vdusek@kpmg.cz

**Filip Horák**

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

**Ladislav Karas**

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

**Ondřej Vykoukal**

Associate
KPMG in the Czech Republic
+420 222 123 660
ovykoukal@kpmg.cz

# Germany

## A. Trial tactics and the right to information according to Art. 15 GDPR

# Trial tactics and the right to information according to Art. 15 GDPR

**The right to be informed and the "right to a copy" according to Art. 15 GDPR has led to considerable discussions within the data protection community. The criticism of an overly extensive interpretation with regard to the scope of this right has echoed particularly loudly from data protection lawyers and their clients. The question acquires a particular significance during ongoing legal proceedings, because the law is sometimes being used more aggressively by individuals in order to gain tactical advantages during a trial.**

**The right to be informed is generally considered to be very extensive but its limits have not been exhaustively discussed.**

- One of the particularly interesting questions is with regard to the wording of Article 15 (3) GDPR ("... a copy of the personal data subject to processing") and it remains unclear which data exactly is covered by the scope of this law.
- While one view assumes that there is a comprehensive right to receive a copy of all existing data (including metadata), the counterview expresses the opinion that only data that has some informational value about the data subject and is currently the focus of processing, is covered by the scope.
- The data protection commissioner of the state of Hesse, for example, states in its activity report as of June 2019 that Art. 15 (3) GDPR generally does not include a claim for copies – for example in the form of a photocopy of certain documents. It would be sufficient "to inform the individual of the personal data contained in a document. However, the copy of a document / e-mail usually does not need to be provided."
- Before that the data protection commissioner of Bavaria also opposed a broad interpretation of Art. 15 GDPR.
- Even the courts have now taken on the question – with different approaches. Where the state labour court of Baden-Wuerttemberg still assumed a comprehensive right to the in-formation of an employee, the district court of Cologne issued a different ruling where it rejected the requirement to produce the copied documents of the person requesting the information.

That being said, the question of how an organization may react to a comprehensive request for information – and in particular during the course of an ongoing trial – is all the more pressing.

## Right to information during civil proceedings

Clients are faced with the challenge that requests for information are often made during pending cases (for example during dismissal protection proceedings before the labour courts). In issuing these requests, individuals ask for copies of all existing data relating to them that the organization has, e.g. employee evaluations, e-mail conversations, messenger chats or log-in data.

- This may result in a considerable amount of time that has to be devoted to assembling all the documents, but this information might also influence an ongoing case.
- The main effect of such a claim might be that the individual has easier opportunities outside of the German Code of Civil Procedure in order to produce evidence in their favour.
- As a consequence, employers, e.g. in pending settlement negotiations, might see themselves in a position to accept an unfavourable settlement due to the pressure generated.

## Possibility to raise objections

**Clients may well have the option to try to object to handing over copies of all the data of the individual, depending on the individual case. Two exemplary arguments could be:**

- The aim of Art. 15 GDPR does not require a copy of all existing data to be transmitted to the data subject. A legality check only requires knowledge of the existence of data and certainly a copy of data containing specific information about the data subject. However, it must be doubted that the concrete information on all personal data, including all metadata, will enable the data subject to examine the legality.
- Another argument might be that if specific copies of such data are required, which concern facts in an ongoing employment dispute or the request is so extensive that obviously pressure on pending negotiations should be exercised, this undermines basic principles of fairness stipulated in Art. 8 para. 2 Charter of Fundamental Rights of the EU and Art. 5 para. 1 lit. a GDPR.
- Interests of third parties might also be taken into consideration as well as objections for disproportionate effort.

Therefore, clients should examine in detail which data must be handed over and which objections may be raised. If the client should decide – in whole or in part – not to comply with the request for information, this decision should be explained and documented in detail with regard to § 34 (2) German Federal Data Protection Act.

# If you have any questions, please let us know

**Maik Ringel**

Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
+49 341 22572-546
mringel@kpmg-law.com

**Nikola Werry, LL.M.**

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

# Georgia

## A. Landmark decision regarding the constitutionality of a block on public access

# Landmark decision regarding the constitutionality of a block on public access

**On 7 June 2019, the Constitutional Court of Georgia rendered a landmark decision regarding the constitutionality of a block on public access to the identities of the parties of litigation in decisions rendered by common courts. The decision established the presumption of publicity for all documents kept at public institutions, and allows limiting access to them only under exceptional circumstances.**

The applicant challenged the constitutionality of several legislative acts, including the General Administrative Code and the Law of Georgia on Personal Data Protection arguing that hiding the names of parties in decisions rendered by Georgian courts at public hearings unreasonably restricts the access to justice of individuals interested in the acts of courts as State institutions.

According to the decision, access to court decisions is an essential component of the transparency of and trust in the judiciary. For this purpose, the public shall have the right to have access to not only the general court practice but also to the full reasoning invoked by a judge when rendering a decision on any specific case.

The Constitutional Court of Georgia considered that access to court decisions is crucial for ensuring public control of and trust towards the judicial system and protecting the right to a fair trial. In the decision, the court also stated that in each individual case when considering the issue of access to a court decision, the effect of personal data disclosure on the privacy of an individual concerned must be evaluated to ensure the maintenance of a fair balance between the public interest and the privacy of individual.

The Constitutional Court decision affects the entire litigation practice in the country. It also gives rise to greater transparency of individual cases and increases the possibility of due diligence and counter-party checks. The new rules shall come into effect from 1 May 2020.

# If you have any questions, please let us know

**Jaba Gvelebiani**

Head of the Legal Department
KPMG in Georgia
+ 995 593 59 55 88
jgvelebiani@kpmg.com

# Greece

A. The first significant fine by the Hellenic Data Protection Authority

B. The Hellenic Data Protection law passed in August 2019

# The first significant fine by the Hellenic Data Protection Authority

**The Hellenic Personal Data Protection Authority imposed on 30 July 2019 the first monetary penalty based on the provisions of GDPR. The penalty, amounting to EUR 150,000 was imposed on a Multinational Auditing Firm (herein the "Company") for unlawfully processing the personal data of its employees.**

According to the complaint filed by the Athens Union of Accounting and Auditors, the Company distributed to its employees a "Statement of Acceptance of Terms of Personal Data", as well as new individual employment contracts which the employees were indirectly forced to sign, given the advantageous position of the employer over the employee.

According to the Data Protection Authority, the Company acting as above violated the principle of lawful, fair and transparent processing of personal data under GDPR Art. 5 paragraph 1 (a) which allows for the use "consent" as a legal basis of processing only if the other legal bases (prescribed in Article 5) are not applicable.

The Company, with its Memorandum, argued that the legal basis of processing was the concluded employment agreements, while consent was requested as an auxiliary basis to reinforce compliance.

In addition, the Company let the employees believe that it was processing their personal data on the legal basis of consent, whereas the processing took place on the basis of another legal basis, unknown to the employees, and breaching in this respect the obligation to provide information pursuant to GDPR Article 13 par. 1(c) and 14 par. 1 ed c).

Finally, the Authority concluded that the Company violated the principle of accountability, pursuant to GDPR Art. 5 paragraph 2, since it failed to provide the Data Protection Authority with internal documentation with respect to the choice of legal basis.

# The Hellenic Data Protection law passed in August 2019

**The Hellenic Data Protection law passed in August 2019.**
**The law for the alignment of Greek legislation to the GDPR was published by the end of August (Law 4624/29).**

## Main provisions for the harmonization of Greek legislation with the GDPR

The new law sets out the scope of the application of the voted provisions, introduces a definition of the terms public and private body, regulates the appointment of Data Protection Officers for public bodies, provides for more specific conditions in relation to the participation of minors to the information society framework, expressly provides for the prohibition of the processing of genetic data for purposes of insurance and health, introduces limitations in relation to the rights of data subjects in cases where their data are being processed by public bodies, introduces provisions for profiling by insurance companies, as well as for the transmission of data between public bodies.

The new law provides for a system of criminal penalties, as well as a special system of administrative penalties for public bodies, according to the explicit provision of the GDPR, whereas it abolishes law 2472/1997, with the exception of specific clauses which are amended and remain in force, concerning amongst others, definitions of terms in relation to the protection of personal data and administrative penalties for violations of the law on electronic services (law 3471/2006).

## Incorporation of Directive 2016/680/EE

The new law, and in the same spirit as the GDPR, sets out the general principles and the scope of the Directive's provisions that are being incorporated into the Greek legal framework.

The law sets out the legal basis for the processing of personal data for a purpose different from the one for which the data has been initially collected. Moreover, the law regulates the process of providing consent, as well as the obligation to maintain confidentiality from the persons involved with the processing of personal data.

Additionally, the rights of subjects (rights on information, access, rectification, complaint) are established and the responsibilities of the controller and processor are defined.

The new law is an important step for the application of the GDPR in Greece, however, there are weaknesses which we expect to be corrected either with amendments to the law or with Decisions and Opinions provide by the Hellenic Data Protection Authority. We will bring you more details in one of the upcoming issues of this newsletter.

# If you have any questions, please let us know

**Kosmatou Liana**

Lawyer/Director
CPALaw
+30 210 60 62 159
lkosmatou@cpalaw.gr

**Vithoulka Penny**

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

# Italy

**A. Facebook fined 1 million Euro by the Italian Data Protection Authority (DPA) within the framework of the Cambridge Analytica case**

**B. Italian Data Protection Authority (DPA) prescriptions on the processing of special categories of personal data**

# Facebook fined 1 million Euro by the Italian Data Protection Authority (DPA) within the framework of the Cambridge Analytica case

**The Italian DPA fined Facebook for infringement on consent and information to data subjects on the basis of the former Italian Privacy Code.**

On June 14, the Italian DPA (Garante per la protezione dei dati personali, hereinafter "Garante") fined Facebook 1 million Euro on account of breaches committed within the framework of the well-known "Cambridge Analytica" case – the latter being the company that had accessed data on 87 million users via a psychological testing app and had used such data to try to influence the US presidential elections in 2016.

The fine was imposed on the basis of the former Italian Privacy Code and it follows up the decision already issued by the Garante in January this year to ban Facebook from further processing the data related to Italian users.

The Garante established that even though only 57 Italians had downloaded the Thisisyourdigitallife app via Facebook's login function, thanks to the sharing of data relating to "friends" enabled by that function, the app had subsequently acquired data relating to an additional 214,077 Italian users who had not downloaded the app in question and who had not been informed of the sharing of their data and had not given their consent to such sharing. Accordingly, the Garante found that Facebook had disclosed the data to the Thisisyourdigitallife app in breach of privacy legislation. However, the data had not been transmitted to Cambridge Analytica.

Facebook was served by the Garante in March this year with a notice of commission of infringements, namely the failure to provide information, obtain consent and reply adequately to the Garante's request for obtaining information and documents. Regarding those infringements, Facebook availed themselves of the possibility to terminate the fining procedure by paying a reduced amount fine of 52,000 Euro.

However, the infringements concerning non-compliance with information and consent requirements had been committed in respect to an especially large, important database, in which case no reduced amount fine may be allowed. In calculating the amount of the fine, the Garante took into account the size of the shared database as well as Facebook's economic status and the number of its users both worldwide and in Italy.

This fine shows the irrelevance of the previous sanctions provided on the basis of the former Italian Privacy Law regarding the protection of personal data against giants like Facebook. In fact, considering the size of the database and therefore the seriousness of the violation, it was only possible to reach 1 million Euro as a fine.

# Italian Data Protection Authority (DPA) prescriptions on the processing of special categories of personal data

**After a public consultation, on 5 June the Italian DPA issued a provision regarding the prescriptions for the processing of special categories of personal data.**

At the conclusion of the public consultation launched last December, the Italian DPA (Garante per la protezione dei dati personali, hereinafter "Garante") adopted a provision ("Provision"), currently published in the Italian Official Journal no. 179 of 29 July, which contains the obligations that must be met by a large number of public and private subjects in different sectors in order to be able to deal with the processing of special categories of personal data as established by article 9 of the GDPR, such as those related to health, political opinions, ethnicity, and sexual orientation.

In fact, the Provision concerns the processing of these particular categories of data in labour relations, the processing of the same data by associative organizations, foundations, churches and religious associations or communities, as well as by private investigators as well as the processing of genetic data and processing activities carried out for scientific research purposes.

The Provision, adopted on the basis of Italian Legislative Decree No. 101/2018 which adapted the national legislation to the EU Regulation, takes into account the most significant and relevant contributions sent by the participants to the consultation.

In the same Provision, the Garante specified that the previous general authorization for the processing of judicial data by private individuals, economic public entities and public subjects (mostly issued at the end of 2016) ceases to produce its effects by not being among the processing activities referred to in art. 21 of the Italian Legislative Decree No.101/2018.

It is also clarified that the general authorizations n. 2, 4 and 5 – concerning, respectively, the processing of data suitable to reveal the health condition and sexual life of the data subject, the processing of sensitive data by freelancers and the processing of sensitive data by different categories of owners – cease to produce their own effects since they are not included in any specific provision of the Italian Legislative Decree No. 101/2018.

# If you have any questions, please let us know


**Dr. Michele Giordano**

Managing Partner
KPMG Studio Associato
KPMG in Italy
+39 055 261961
michelegiordano@kpmg.it

**Atty. Paola Casaccino**

Attorney-at-law
Senior Manager Governance
Risk & Compliance Services
KPMG Studio Associato
KPMG in Italy
+39 055 261961
pcasaccino@kpmg.it

**Atty. Alessandro Legnante**

Attorney-at-law
Senior Legal Specialist
Risk & Compliance Services
KPMG in Italy
+ 39 055 2619691
alegnante@kpmg.it

**Atty. Giulio Grasso Cannizzo**

Attorney-at-law
Senior Legal Specialist
Risk & Compliance Services
KPMG in Italy
+39 055 261961
ggrassocannizzo@kpmg.it

# Poland

A. Polish national legislation on Personal Data Protection

B. Statistics for 2018

C. The first fine imposed by the Office

D. News and opinions from the Office

E. The Office recommendations based on the Fashion ID Case

F. A warning about mobile apps

# Polish national legislation on Personal Data Protection

**In May 2018, a new Polish Personal Data Protection Act, issued in connection with GDPR regulations (the "Act"), came into force. The Act regulates, among others, the status and activities of the President of the Office for Personal Data Protection (the "Office"), including the rules regarding official inspection. The Act provides regulations related to the appointment of DPO by controllers and its registration with the Office, certification mechanism, professional codes, as well as administrative and criminal penalties for the violation of personal data protection provisions.**

**Irrespective of the above, at the beginning of May 2019, the Act amending certain particular acts in connection with the application of GDPR came into force. The Act amended approx. 170 particular acts. The most important changes apply to the Labour code:**

1. The legal basis for processing personal data in the recruitment process is now (among others) the controller's legal obligation (Article 6. 1. c) GDPR),
2. The employer may also process the personal data of the applicant or employee based on their consent (excluding information on convictions and violations of law),
3. There is a new catalogue of required personal data in the recruitment process,
4. The Act obliges the employer to issue a written authorization for persons processing the employees' sensitive data.
5. It provides specific regulations concerning the surveillance (monitoring) of employees.

The Act also confirms the status of attorneys-at-law and tax advisors as data controllers. In the field of banking and insurance law, additional rights for consumers are provided. At the request of the consumer applying for a loan, the bank will present to him/her the factors, including personal data, which have had an impact on the creditworthiness assessment.

# Statistics for 2018

Approx. 20 inspections were performed by the Polish Office for the Protection of Personal Data.

Approx. 4000 complaints were received by the Office for the Protection of Personal Data.

No fines were imposed in 2018 (in 2019 there were two fines imposed).

The highest fine was approx. PLN 1,000,000 (app. EUR 235,000).

# The first fine Imposed by the Office

**In March 2019, the President of the Office imposed a fine in the Office for Personal Data Protection (the Office) amount of approx. PLN 1,000,000 on a credit information agency (a company creating databases re. persons running business activities). The source of the data incorporated in the databases created by that company was information included in public databases, such as the National Business Register, Central Register and Information on Business Activity or data published by the Statistical Office. The fine was imposed due to the fact that the company in question did not inform a considerable number of data subjects, based on Article 14 GDPR, that their personal data had been obtained and did not transfer the mandatory information on the conditions of their data processing.**

The company explained that it did not distribute the necessary information due to the excessive costs (disproportionate effort) that would be generated if they were sent (they allegedly may have amounted even to PLN 30,000,000). Instead, the company published this information on its website. The Office did not deem the above explanation to be satisfactory and imposed the fine in question. According to the Office, the company should have distributed the information based on Article 14 GDPR to particular data subjects, e.g. via letter or sms. An important factor in the assessment of the case was the fact that the company in fact had the data of the data subjects concerned. In other words, according to the Office, only in the case that the company did not have this data, their obtaining of it might be qualified as a disproportionate effort within the meaning of Article 14. 5. b) GDPR).

# News and opinions from the Office

A new Act on public documents has been introduced, prohibiting the copying of Public Documents such as an ID or driver's license, in case a copy (replica) has the characteristics of authenticity of such documents. In the opinion of the Office for Personal Data Protection ("the Office"), not all copying is prohibited (eg. an ordinary black and white copy of an ID does not have characteristics of authenticity) but it shall be submitted to a minimalization rule. The Office recommends collecting statements with required information instead of the copying public documents.

The Office seeks to ensure that the PESEL number is not public in the electronic signature certificate or used as an identifier in digital services. The Office proposes, therefore, that the Ministry of Digitization should limit the publication of PESEL while working on further regulations to counter identity theft. The Ministry of Digitization has declared its intent to continue its efforts in this manner.

In the Office's opinion employers are not entitled to independently check the sobriety of employees as they process sensitive data during such verification. The content of the Act on Upbringing in Sobriety and Counteracting Alcoholism precludes random or preventive testing of breathalysers. The opinion was criticized by the representatives of employers as well as data protection specialists. There is a movement to change the law in this matter to authorize employers, especially in transport and construction, to conduct such sobriety tests.

# The Office recommendations based on the Fashion ID Case

Based on the European Court of Justice's judgment in the Fashion ID case, the Office reminds entities using Facebook social plugins such as "Like"buttons to fulfill the information Office for Personal Data Protection (the Office) obligation towards persons using websites. A visitor to such a site must know that the operator transmits its data to Facebook. Personal data is information about the user's IP address and browser ID.

The web administrator needs to have a premise for the processing of personal data in the field of transmission of these data to the Facebook social portal (consent, legitimate interest).

The Office recommends including in the security policies the information about transferring personal data to Facebook in connection with the use of the "Like" plugin.

# A warning about mobile apps

**The Office warns about using mobile apps such as FaceApp. The Office recommends verification of:**

- what data and functions of our device the app wants to have access to,
- whether the scope of data transmitted through it is adequate for the purpose for which the application was created,
- whether the information notice (clause) required under GDPR is provided,
- whether it is really necessary to grant any additional consents for data processing by the app,
- the source of the app, if it is provided by an official distributor.

# If you have any questions, please let us know

**Magdalena Bęza**

Senior Associate
KPMG in Poland
48 22 528 14 05
mbeza@kpmg.pl

**Natalia Kotłowska**

Associate
KPMG in Poland
48 61 845 46 80
nkotlowska@kpmg.pl

# Romania

## A. Data Protection news: first fines imposed by the Romanian DPA

# Data Protection news: first fines imposed by the Romanian DPA

**In Romania, the latest developments from a personal data protection perspective occurred during July and August when the first fines were imposed.**

**The sanctions are as follows:**

1. On the 27 of June 2019, the Romanian National Supervisory Authority for Personal Data Processing (hereinafter referred to as the "NSAPDP") finalized an investigation at a Romanian Bank and found that it breached the provisions of art. para 25 (1) of the GDPR. The controller was sanctioned with a fine in the amount of RON 613,912, representing the equivalent of EUR 130,000. The sanction was applied as a result of the failure to implement appropriate technical and organizational measures, both within the determination of the processing means and processing operations themselves, designed to effectively implement data protection principles, such as data minimization, and to integrate the necessary safeguards in the processing, in order to meet the GDPR requirements and to protect the rights of the data subjects.
2. On the 2 July 2019, the NSAPDP completed an investigation into a Romanian Hotel and found that it infringed the provisions of art. 32 para. (4), art. 32 para. (1) and para. (2) of the GDPR relating to the security of processing. The controller has been sanctioned with a fine amounting to RON 71,028, representing the equivalent of EUR 15,000.
3. On the 5 July 2019, the NSAPDP completed an investigation and found that the controller infringed the provisions of art. 32 para. (1) and para. (2) of the GDPR. The controller was sanctioned with a fine in the amount of RON 14,173.50, representing the equivalent of EUR 3,000. The sanction was applied to the controller as it did not implement appropriate technical and organizational measures in order to ensure a level of security appropriate to the risk of processing. This resulted in the unauthorized disclosure and unauthorized access to the personal data of persons who have performed transactions received by the website (name, surname, mailing address, email, telephone, workplace, details of transactions made), contained in publicly accessible documents, between the 10 December 2018 and the 1 February 2019.
4. Also, in July 2019 an investigation by the NSAPDP was completed, and the controller subject to investigation was sanctioned with a fine amounting to RON 11,834.25, representing the equivalent of EUR 2,500, respectively:
   - A fine of RON 4,733.70 (equivalent to EUR 1,000) for the violation of the provisions of art. 12 of the GDPR and
   - A fine of RON 7,100.55 (equivalent to EUR 1,500) for the violation of the provisions of art. 5 para. (1) lit. c) corroborated with art. 6 of the GDPR.

**The sanctions were applied by the NSAPDP due to the fact that the controller:**

- could not prove that data subjects had been informed about the processing of personal data/images through the video surveillance system, beginning in 2016;
- performed the disclosure of the personal identification number (CNP) of the employees by displaying a report of the authorized personnel (having a specific certification) to the company's bulletin board and was unable to prove the lawfulness of the processing of the personal identification number by disclosure, according to art. 6 GDPR.

The controller was obliged to take appropriate measures to provide the data subject with any information note referred to in art. 13 and 14 from the GDPR.

# If you have any questions, please let us know

**Laura Toncescu**

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

**Adrian Lincă**

Legal Consultant
KPMG in Romania
+40 (728) 008 138
alinca@kpmg.com

# UK

A. New ICO guidance on Cookies

B. The UK DPA announces its intention to levy first major fines under the GDPR

# New ICO guidance on Cookies

**The UK's data protection regulator, the Information Commissioner's Office ("ICO"), released new guidance in July for companies using cookies, and similar technologies, used for storing information and accessing stored information on users' devices. The ICO also makes an attempt to update its guidance with regard to more recent technologies such as wearable tech and the Internet of Things ("IoT"). Such devices will be considered subject to the rules for cookies and the regulator advises makers to consider how best to ensure users can be informed of the presence of cookies on IoT devices when the physical interfaces on them are often limited or non-existent.**

This guidance was released to align the ICO's approach with the GDPR. Although cookies primarily come under the Privacy and Electronic Communication Regulations ("PECR"), there are important concepts in PECR, such as consent and transparency, which must now be interpreted in line with GDPR. In addition, PECR can operate in an area where GDPR provisions also apply, as the use of cookies can frequently involve the processing of personal data.

**Points to note from the ICO's guidance include:**

1. Confirmation that consent must be obtained for the purposes of setting cookies (except as exempted in PECR) and that this must be in accordance with GDPR. The following should be borne in mind:
   - Users must take clear, positive action (continuing to browse the website is not sufficient).
   - Users must be able to select which cookies they do or do not wish to consent to (i.e. those for some purposes vs those for others). Thus users must be presented with enough clear information to understand what the cookies are for, as well as the option to distinguish between them.
   - No pre-ticked boxes or sliders set to "on". The default setting should allow no cookies, leaving it to the user to definitively choose and take action to consent. This is in line with the EU Advocate General's view in a case earlier this year, which also makes clear that cookie consent options should be separate and distinct, with their own tick box or slider and on an equal footing with any other consents required from the user for the site.

2. Following on from point 1, the ICO confirms that consent will be required for all cookies, bar those specifically exempted in PECR that are strictly necessary for the purposes of facilitating communications, or providing certain services. The ICO goes on to note that, where the exemptions do not apply, and consent is required; to the extent that GDPR also applies (because personal data is being processed) consent shall form the only lawful basis available for processing under GDPR. This means attempts to cite "legitimate interests" as a basis for avoiding the need to obtain consent for cookies is unlikely to work.

3. The ICO advises organizations to conduct a "cookie audit" and review their existing online services on a regular basis:
   - Once existing cookies are identified, they should verify how compliant they are with existing regulations, assessing whether they are necessary and proportionate, and what steps they have taken to inform users and to obtain their consent.
   - The ICO will never exclude the possibility of formal action, but has indicated that priority would not be given to uses of cookies where there is a low level of intrusiveness and low risk of harm to individuals. They are more likely to focus on cookies perceived to be highly intrusive such as those used to support profiling for direct marketing purposes.

## Associated developments across the EU

**The guidance is consistent with developments across the EU in this area, e.g.:**

- In the same month as the ICO, France's regulator, the Commission Nationale de l'informatique et des libertés ("CNIL"), also released new guidance to align the application of PECR with the GDPR. One focus of the new guidelines was a clarification of how valid consent will be defined. Echoing the ICO's guidance above, simply scrolling down or swiping onwards on a website or app will no longer be sufficient to constitute consent. Consent must be an unambiguous, positive action, taken freely on the basis of specific and clear information.
- Earlier in the year in February, the Dutch DPA, the Autoriteit Persoonsgegevens ("AP") responded to complaints from users about so-called "cookie walls". These are essentially demands that visitors to a site consent to have their browsing tracked to facilitate targeted advertising; users who do not give their consent are denied entry to these sites. The guidance released by the AP clearly set out its view that attempting to barter data in exchange for access to a website was in breach of the GDPR's requirements for free and informed consent. The AP stated that they expected sites to stop this practice as soon as possible.

## Conclusion

Although this is updated guidance, rather than new law, the clarifications are very useful. The ICO has updated its own cookie consent mechanism and we note that many organizations have been updating theirs in order to comply. However, this area will continue to change. The finalised text of the new EU ePrivacy Regulation is awaited with interest. This is a piece of European legislation that is currently under development, which is intended to replace the European legislation on which PECR is based and aims to update and modernise the law in this area.

# The UK DPA announces its intention to levy first major fines under the GDPR

**In early July the Information Commissioner's Office ("ICO") announced its intention to impose fines of £183.39 million and £99,206,396 on two multinational companies in respect of GDPR infringements. The first incident was reported to the ICO in September 2018 and involved the personal data of approximately 500,000 customers being compromised in a cyber incident. In the second incident, the personal data contained in approximately 339 million customer records was exposed following a cyber incident. Of these records, around 30 million related to residents of 31 countries in the European Economic Area.**

The first incident in part involved user traffic to the company's website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. The ICO announced its intention to impose the fine in response to a statement made to the London Stock Exchange. Following the announcement the Information Commissioner, Elizabeth Denham issued a strong message, stating, "People's personal data is just that – personal. When an organization fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it…"

The second incident emphasises the importance of ensuring due diligence conducted during an acquisition includes an analysis of the cyber security measures in place at the target company. In 2016 the company in question had acquired another group, where it is believed a vulnerability in systems had begun in 2014. The exposure of customer information was not discovered until 2018. The ICO's announcement was made in response to a filing with the US Securities and Exchange Commission by the company. Its investigation found that the company had failed to undertake sufficient due diligence when it made the acquisition in 2014 and should also have done more to secure its systems.

## Conclusion

The size of the fines is not settled yet, and may either increase or decrease as these cases develop. In both cases the ICO will be considering representations from the companies involved, as well as from other DPAs around Europe, on whose behalf it effectively acts as the lead supervisory authority under the GDPR's "one stop shop" provisions. Both companies have cooperated with the ICO's investigations and taken steps to improve their security measures, something which has been shown, in other EU jurisdictions, to potentially mitigate the size of the fine, and which is also mentioned in the ICO's Regulatory Action Policy ("RAP") as being a mitigating factor. However, the RAP also makes note of the importance of bearing in mind the public interest and ensuring its actions are an effective deterrent against future breaches. The ICO's final decisions will give an indication of how the ICO balances the mitigating factors against the criteria set out in its RAP, including consideration of the public interest. The level of the indicated fines has already attracted much attention and serves as a reminder of the importance of respect for privacy as required by compliance with GDPR.

# If you have any questions, please let us know


**Lucy Jenkinson**

Solicitor, ISEB (Data Protection)
KPMG in the UK
+44 (0) 131 527 6823
Lucy.Jenkinson@KPMG.co.uk

**Lydia Simpson**

Barrister, BCS (Data Protection)
KPMG in the UK
+44 (0) 7810056806
Lydia.Simpson@KPMG.co.uk

**William Beresford Davies**

Paralegal, Legal Services
KPMG in the UK
+44 (0) 203 078 3634
William.BeresfordDavies@kpmg.co.uk

# Vietnam

## A. Law on Cybersecurity

# Law on Cybersecurity

**On June 12, 2018, the Vietnamese National Assembly passed the Law on Cybersecurity ("CSL") which took effect on January 1, 2019. CSL seeks to protect national security and ensure social order and safety by regulating activities in cyberspace.**

Previously, these activities were regulated by a myriad of regulations such as the Penal Code, Law on E-Transactions, Law on Information Technology, Law on Cyber Information Security, and the Law on Telecommunications, all of which principally governed the collection, use and handling of personal data.

## Scope

The CSL applies to both local and foreign entities, agencies and individuals who provide services in telecommunications, the internet and other value-added services on the internet in Vietnam. It is broad in scope and appears to cover any businesses whatsoever as long as the services are delivered via a network environment.

## Prohibited acts in cyberspace

**In addition to the usual prohibitions (such as cyberattacks, obstructing computers or telecommunication networks or unauthorized intrusion against the authorities in performing their duties), some of the acts prohibited under the CSL include:**

1. Distorting of history, negating revolutionary achievements, undermining national solidarity, offending religions and engaging in racial and gender discrimination;
2. Providing false information to confuse netizens, causing harm to socio-economic activities, obstructing or impeding the activities of the state authorities or people performing public duties and violating the lawful rights and obligations of other organizations and individuals;
3. Activities involving prostitution, social vice, human trafficking, posting pornographic or criminal material, destroying the country's fine traditions and customs or social morality and public health;
4. Inciting or enticing others to commit crimes;
5. Carrying out cyber espionage and unauthorized intrusion into State secrets and personal information on cyberspace;
6. Organizing, colluding, inciting, bribing, cheating or training people to oppose the government.

Although most of these prohibitions are further defined/clarified in the subsequent articles of CSL, the language of the law is still broad, permitting the state authorities significant discretion. Also, the administrative penalties for breaches of any of the listed prohibitions will be clarified in implementation guidelines that have yet to be developed.

## Salient requirements under the CSL

The CSL creates several onerous obligations on the part of covered entities.

**Data localization and retention of personal data**
Firstly, the CSL requires covered entities to comply with the data localization requirement. Under this law, the covered entities are required to store personal data of Vietnamese users for a prescribed period of time. The retention period, the scope of the data to be stored (i.e. only a copy or all of the data), and the covered organizations are subject to further guidance by the government. In addition, companies must provide information to authorities about their user when such user is being investigated or deemed to have breached the CSL.

**Requirement to comply with disclosure requests made by the authorities**
All organizations are mandated to surrender user information to the authorities upon receipt of a written request. This obligation extends to access to the entity's information system for serious breaches. It is not clear if the authorities can bypass the data owners and approach third party service provider services (such as cloud service providers) directly.

**Content control**
Another significant provision of the CSL is the requirement that domestic and foreign companies supervise user posts and comply with any request from the authorities to delete data that is deemed illegal or prohibited. The request could potentially include other remedial measures such as banning the data user from accessing the covered entity's services in the future. Thus far, one social media company was announced to have violated the regulations on content control and delayed removing anti-government content despite receiving a removal request from the authorities.

**Commercial presence**
The CSL also requires foreign companies to establish a branch or a representative office in the country through its commercial presence requirement. This provision enables the enforcement of the CSL against foreign entities. However, the draft decree released on 31 October 2018 seems to limit the requirement to entities that have allowed users to conduct acts that compromise national security and public order, or distort history.

## Legal consequences for non-compliance

Companies may be liable for disciplinary or administrative penalties, or commit a criminal offence when failing to comply with CSL, based on the nature and degree of violation. Of note is the absence of recourse for covered entities who take a different opinion from the authorities. The CSL makes the authorities the final adjudicator of what content is deemed illegal. At present, the CSL is quite like a policy document specifying obligations and requirements in broad terms. The government will be issuing further legal instruments to guide its implementation. Therefore, individuals and organizations will need to monitor ongoing developments to understand their obligations under the CSL.

# If you have any questions, please let us know


**Richard Stapley-Oh**

Partner
KPMG in Vietnam
+84 28 38219266
rstapleyoh@kpmg.com.vn

**Nguyen Thi Hoang Trang**

Manager
KPMG in Vietnam
+84 28 38219266
tranghnguyen1@kpmg.com.vn

**Amarjit Kaur**

Manager
KPMG in Vietnam
+84 28 38219266
amarjitsingh@kpmg.com.vn

September 2019