Data privacy newsletter

KPMG Global Legal Services

April 2022

Contents

Spain

A First sectoral code of conduct approved by the AEPD

The code of conduct, promoted by Farmaindustria (Spanish Business Association of the Pharmaceutical Industry), responds to the application of data protection regulations in clinical and biomedical research, as well as in pharmacovigilance.

Codes of conduct are voluntary compliance mechanisms that establish specific rules for categories of controllers or processors in order to contribute to the correct application of the applicable data protection regulations. The GDPR sets them up as an instrument of compliance with the accountability principle and requires to be approved by a competent supervisory authority. In this case, the Spanish Data Protection Commissioner (AEPD).

The topics that are regulated in this code of conduct include the application of data protection principles within the clinical and biomedical research, the performance of impact assessments, data anonymization, the role of the different participants in a clinical trial, the applicable legal basis for processing personal data (please note that as a general rule, it is set forth that consent would not be the appropriate legal basis to process the personal data of the participants), the international data transfer regime, the obligations derived from security breaches and procedures for the exercise of rights by data subjects.

Finally, we would like to highlight that the code of conduct provides with a template of the information to be provided to participants in a clinical trial to comply with the transparency principle set forth by the GDPR as well as a template of the data protection clauses to be included in the agreements to be subscribed by the sponsor and/or the centre with the different third parties that they will use and that will act as data processors of the formers.

B The AEPD clarifies how to file data subject rights related to unsolicited commercial communications

The Spanish Data Protection Commissioner (AEPD) provides recommendations to avoid receiving unsolicited commercial communications.

Despite acting conscientiously when providing our personal data to data controllers, (not providing our consent for the processing of our personal data for advertising purposes, registering in the Robinson List, etc.) it is still possible that we receive unsolicited commercial communications via phone calls, email, etc. The AEPD has provided several recommendations to prevent receiving such unwanted advertising.

Firstly, it is recommended to follow the methods provided in each electronic communication for rejecting the use of data for advertising purposes (sending an email, SMS, clicking the provided link or calling a free telephone number are common means provided to

unsubscribe from receiving commercial communications). If we continue receiving commercial communications, we should use the channels established by the company itself for exercising our data protection rights. In many cases, the data subject will have the option to revoke his consent when the data processing is based on this legal basis (Article 6.1 a GDPR). The data subject may also exercise his right to object to the processing of personal data when the data processing is based on the data controller's legitimate interest.

If none of these options have results, data subjects can contact the company's data protection officer or even address the AEPD to file a formal complaint.

The AEPD publishes a checklist to help data controllers carry out Privacy Impact Assessments

The Spanish Data Protection Commissioner (AEPD) has published a checklist of items to help data controllers identify and determine if the process and documentation followed to carry out Data Privacy Impact Assessments (PIAs) contain all the elements required by the applicable regulations.

This checklist complements the guide issued by the AEPD 'Risk management and impact assessment in personal data processing' and allows, once the PIA has been developed and documented, to carry out a final check to ensure that all the aspects included in the data protection regulations have been taken into account.

The GDPR establishes that organizations that process personal data must carry out risk management programs in order to establish relevant measures to guarantee the rights and freedoms of individuals. In addition, in those cases in which the data processing implies a high risk for data protection, the GDPR provides that these organizations are obliged to carry out a PIA to mitigate those risks. If after conducting the PIA, and after having adopted measures to mitigate the risks for data subjects' rights and freedoms the risk is still high, the data controller must file a formal consultation with the AEPD before carrying out this processing of personal data.

The objective of this new resource of the AEPD is to help data controllers to comply with the obligations of developing and documenting PIA and so that, in the event of having to file this prior consultation with the AEPD, it is easier to verify that the consultation complies with the applicable requirements for its presentation.

Contact

If you have any questions, please let us know

Noemí Brito
Director
KPMG in Spain
T: +34 91 456 34 00
E: noemibrito@kpmg.es

Eric Romero
Senior Manager Lawyer
KPMG in Spain
T: +34 93 253 29 03
E: ericromero@kpmg.es

Claire Murphy
Manager Lawyer
KPMG in Spain
T: +34 91 456 34 00
E: clairemurphy3@kpmg.es

David Manuel Navarrete
Lawyer
KPMG in Spain
T: +34 699 75 66 15
E: davidmanuelnavarrete@kpmg.es

Belgium

TCF System not GDPR compliant

The Belgian DPA recently fined an international digital marketing organization for non-compliance with GDPR.

On 2 February 2022 the Belgian Data Protection Authority (DPA) ruled that the Transparency and Consent Framework (TCF) developed by an international digital marketing organization did not comply with several provisions of the General Data Protection Regulation (GDPR). The DPA imposed a fine of 250.000 EUR and required an action plan for compliance with the GDPR in two months.

TCF is a widespread mechanism that facilitates the management of user preferences for online personalized ads. It reflects processing purposes and user preferences with respect to potential vendors, aiming to strengthen the GDPR compliance of organizations by relying on the so called OpenRTB protocol.

This protocol is used very frequently for "Real Time Bidding". When users visit a website or application that contains ad space, technology companies, representing thousands of advertisers, can bid for that ad space "in real time" behind the scenes through an automated auction system that uses algorithms to show targeted ads tailored to the visitor's profile.

An interface (Consent Management Platform) appears upon first visit of a website or application where users can give their consent or objection to the collection and sharing of their personal data or the various types of processing, which happen based on the legitimate interests of ad tech vendors.

TCF captures the users' preferences, which are then encoded and stored in a "TC string" (Transparency and Consent String). These preferences are shared with the organizations participating in the OpenRTB system, giving them knowledge of the users' consent and objections. The CMP also places a cookie on the user's device. This cookie, in combination with the TC string, can be linked to the user's IP address, making the user identifiable.

The Belgian DPA considered that the international digital marketing organization acted as a data controller with respect to the registration of the destination signal and the users' preferences and objections by means of the unique "TC string", which is linked to an identifiable user.

Following this conclusion, the Belgian DPA found some violations of the GDPR. Regarding the lawfulness of the processing, the Belgian DPA stated that the international digital marketing organization has no legal basis for the processing and that the legal grounds provided by TCF for further processing by ad tech vendors were insufficient. Furthermore, the information provided through the CMP interface was considered too general and vague to understand the nature and scope of the processing, making it (too) difficult for users to retain control over their personal data.

Furthermore, a number of other violations of the GPDR, such as the fact that no register of processing activities was drafted, no data protection officer was appointed and no data protection impact assessment was conducted, were established.

Given the risk that a large group of citizens might lose control over their personal information, the Belgian DPA has imposed an administrative fine of €250,000 in addition to corrective measures (including establishing a valid legal basis and thoroughly screening participating organizations on GDPR issues) to make the current version of the TCF compliant under GDPR.

It is worthwhile mentioning that, in the light of the "one-stop shop" mechanism (the cooperation mechanism under the GDPR), the current decision was approved by all authorities involved.

B

Fine for mass processing of social media data in connection with the Benalla affair for political profiling

The Belgian Data Protection Authority (DPA) recently fined an NGO and its researcher for publishing raw and sometimes sensitive data from social media accounts as part of an investigation.

The NGO, which aims to combat the spread of disinformation, published an analysis in 2018 to determine the possible political origin of tweets circulating about the 'Benalla affair'. The GBA and its French counterpart, the CNIL, received a total of more than 200 complaints about:

- the re-use of personal data from 55.000 social media accounts to carry out the study (in which more than 3.300 accounts were politically classified); and
- the online publication of files containing the raw data of the study (including information on the religious beliefs, ethnic origin, and sexual orientation of the persons whose accounts were analyzed).

As the NGO is based in Belgium, the Belgian DPA is responsible for the matter and made the decision in collaboration with the CNIL. The Belgian DPA decided that the NGO was exempt from its obligation to inform the persons individually about the personal data processed for the study, as this could have jeopardized the study and its publication. The Belgian DPA, however, finds that the publication of sensitive data used for the study - which was not properly pseudonymized - had no legal basis due to the disproportionate infringement of the rights of the authors of the tweets concerned. The Belgian DPA also stated that their consent was required for the publication of such non-pseudonymized sensitive data.

The Belgian DPA concludes that the data controller did not comply with various obligations under the GDPR. Balancing the right to journalistic freedom of expression and the right to data protection was not possible given the very large number of social media accounts involved. The Belgian DPA therefore decided to fine the NGO 2.700 EUR and the investigator 1.200 EUR, and to issue a reprimand.

The Belgian DPA emphasized that compliance with the GDPR is essential in the context of the large-scale collection of data for political profiling, and its publication, which may have adverse effects on individuals.

An important take-away from this decision is that publicly available data also falls under the protection of the GDPR. Hence, the fact that you have shared something publicly does not mean that you just have to accept any subsequent re-use.

[1]Alexander Benalla, the former employee of President Emmanuel Macron, was discredited after the newspaper Le Monde revealed that he had dealt harshly with protesters at the 2018 May 1 celebrations.

Contact

If you have any questions, please let us know

Frank Cleeren
Partner
KPMG Law Belgium
T: +32 (0)11287977
E: fcleeren@kpmglaw.be

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

Laura Vanuytrecht
Senior Associate
KPMG Law Belgium
T: +32 (0)11287961
E: lvanuytrecht@kpmglaw.be

Germany

Germany implements the last parts of the EU ePrivacy Directive (from 2009

The German legislator finally implemented rules on 'Cookie'-consent in line with the ePrivacy Directive (2009/136/EC) from 2009 following the judgement "Planet49" by the European Court of Justice in 2019 (C-673/17) and the German Federal Supreme Court Ruling from 2020 (I ZR 7/16).

On 1 December 2021 the Federal Act on the Regulation of Data Protection and Privacy in Telecommunications and Telemedia ("TTDSG") entered into force. This relatively short piece of legislation focuses on two areas: (i) It bundles the essential data protection regulations for telecommunications and telemedia services into one Act, and (ii) it regulates the consent requirement under Article 5 (3) of the EU Directive (2009/136/EC) ("ePrivacy Directive"). With the TTDSG the German legislator closed the legislative gap and implemented the lacking `Cookie`-consent provisions

The new requirements almost fully mirror the wording of the Directive and clarify what was already current market standard based on the relevant case law of the German Federal Court of Justice. In particular, that website operators must obtain active and informed prior consent from each visitor if their website uses cookies or similar tracking tools. This consent requirement applies to any device connected to the internet (e.g. cars, televisions and smart devices) provided information is stored on or accessed from it regardless of the information being personal or non-personal data.

Exceptions apply whenever the used technology is "strictly necessary" for the requested service e.g. the functioning of the website or device. This means that the German regulator refrained from providing any clarification on the long-lasting and intense debates on what falls under the opaque term "strictly necessary". In particular, if statistical or similar services are classified as strictly necessary or not. And thus, leads to the continuous requirement of case-by-case assessments.

Furthermore, a new concept implemented by the TTDSG is the option of neutral third-party personal information management systems (PIMS) that uniformly manage user consents making cookie banners obsolete. Such PIMS are subject to the caveat that the federal government issues an additional legislative decree that regulates more details which is not in sight at the moment.

The consent requirement, regardless of the processing of personal or non-personal data, has an extensive territorial scope applying to all companies with an establishment in Germany, or that provide services or goods in Germany. Finally, any infringements of the TTDSG-consent requirements can be sanctioned with fines up to EUR 300,000 and the data protection authorities are expected to noticeably intensify their sanctions practice.

From a practical point of view the adaption by the German legislator finally closes an obvious gap but has limited practical relevance as it mirrors the existing case law. However, it lacks clarification on how to deal with statistical or similar "strictly necessary" services but brings an end to the grace period of imposing fines by

the German authorities. This makes it even more critical for any website operators to closely implement the required processes and to monitor the development of the legal situation at EU level. Mainly because the draft of the long-planned ePrivacy Regulation which was supposed to replace the ePrivacy Directive contains essential amendments in respect of the 'Cookie'-consent requirement and the use of tracking technologies.

Furthermore, the draft of the EU Data Governance Act provides for a notification procedure for providers of PIMS and could bring lasting changes to the modalities for obtaining consent.

B

German courts rule on claims for damages under the GDPR

German courts are increasingly ruling on claims for damages by data subjects. Especially two questions seem to have a high significance: whether data subjects should be compensated for non-material damages at all and whether the damage needs to have a certain minimum impact.

Current decisions for and against damage claims

In addition to administrative fines for data protection violations, natural persons can also claim damages in the event of a GDPR violation. Under Art. 82 of the GDPR, data subjects have their own claim for damages against data-processing companies if they have suffered damage as a result of a GDPR breach. Claims for damages by individuals may seem negligible compared to a high fine imposed by the authorities. However, when you consider that GDPR breaches often affect large data sets and thus frequently thousands or even hundreds of thousands of individuals, the picture is different. The individual damages can accumulate and quickly reach or even exceed the total fine risks.

In some cases, courts only assume non-material damage if a violation of data protection law in an individual case has led to a concrete, not merely insignificant or perceived violation of personal rights. In the past, German courts have been rather reluctant to award compensation for non-material damages under Art. 82 GDPR. However, some more recent decisions - in particular those of the labor courts - show a different tendency.

The Dresden Higher Regional Court (4 U 1158/21) awarded the affected party damages in the amount of 5,000 euros. The person concerned had been shadowed by a detective whose task was to find out whether the person concerned had committed a criminal offense in the past.

The court stated that:

- the impairment must exceed a de minimis threshold,
- for the estimation of damages, among other things, the nature, gravity, and duration of the infringement must be taken into account, and
- according to the principle of effectiveness (effet utile), a deterrent sanction is not excluded; this does not mean that the monetary compensation must necessarily have a punitive character.

The Regional Court of Cologne (5 O 84/21) on the other hand denied a claim for damages with the following argumentation:

- A breach of the GDPR is not sufficient to justify a claim; rather, damage must also have been incurred.
- A reversal of the burden of presentation and proof is only to be expressly inferred with regard to the aspect of fault; otherwise, the general civil law rules on the allocation of the burden of proof apply which means that the plaintiff must prove both the GDPR infringement and its damage.
- The intended deterrent effect can only be achieved through damages for pain and suffering that are severe for the defendant; this applies in particular if there is a lack of "commercialization" with respect to the processed data; awarding damages for pain and suffering in a minor case would entail the risk of a boundless accumulation of the assertion of claims,

which does not correspond to the purpose of Art. 82 GDPR.

Also, the Bremen Higher Regional Court (1 W 18/21) rejected a claim for damages with the argument that it was not sufficient to allege a breach of the provisions of the GDPR without submitting a claim for non-material damage caused thereby.

Referrals to the ECJ

In a referral to the European Court of Justice, the German Federal Labour Court (8 AZR253/20(A)) deals with various open questions regarding Art. 82 GDPR. The court presented the following important and essential questions to the ECJ for a preliminary ruling in the course of the proceedings:

Art. 82 (1) GDPR: Does the provision have a special or general preventive character and must this be taken into account when assessing the amount of the non-material damage to be compensated at the expense of the controller or processor?

Does the degree of fault matter when assessing the amount of damages? In particular, may non-existent or minor fault on the part of the controller or processor be taken into account in its favor?

In addition, the order for reference contains the following judicial findings:

The claim for non-material damages under Art. 82(1) GDPR does not require the injured person to show non-material damage suffered; the data subject also does not have to show a consequence or consequence of the infringement of at least some weight.

The violation of the GDPR itself leads to a non-material damage to be compensated for.

The liability of the controller (or processor) under Art. 82(1) GDPR is strict; the provision cannot in any way make the liability of the author of the breach dependent on the existence or proof of fault.

The Regional Court Saarbruecken (5 O 151/19) referred the following questions to the ECJ for a preliminary ruling:

Art. 82(1) GDPR: Is the concept of non-material damage to be understood in the sense that it covers any impairment of the protected legal position, irrespective of its other effects and their materiality?

Art. 82(3) GDPR: Is liability excluded by attributing the infringement to human error in the individual case of a person subject to Art. 29 GDPR?

Is it permissible or advisable to base the assessment of non-material damages on the assessment criteria set out in Art. 83 GDPR for fines?

Is the compensation to be determined for each individual infringement or are several infringements sanctioned with an overall compensation?

The answer to these questions will be essential for the German courts. Until then, many questions will be judged differently by the courts.

Conclusion

Overall, it can be said that Art. 82 GDPR is understood relatively narrowly in German case law and many courts do not recognize a claim for damages in every infringement.

For some months now, however, there has been a trend in case law towards higher awards for damages in the event of GDPR violations. The courts are interpreting Art. 82 GDPR broader. Some courts even assume that the damages to be awarded to the plaintiffs must have a deterrent effect or reach a deterrent amount. This development may have significant financial and other consequences for data processing companies as data breaches and other violations of data protection law often affect more than just one individual.

Contact

If you have any questions, please let us know

Francois Heynike, LL.M. (Stellenbosch)
Partner
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49-175-6432054
E: fheynike@kpmg-law.com

Sebastian Hoegl, LL.M. (Wellington)
Senior Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49 172 7447629
E: shoegl@kpmg-law.com

Leonie Schönhagen, LL.M. (Edinburgh)
Manager
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49 151 15692057
E: lschoenhagen@kpmg-law.com

Sandra Zeis
Senior Associate
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49 170 4192101
E: szeis@kpmg-law.com

Pia Neuhaus
Senior Associate
KPMG Law Rechtsanwaltsgesellschaft mbH
T: +49 151 61264491
E: pneuhaus@kpmg-law.com

Romania

Romania takes third place in the EEA for number of GDPR fines in 2018 – 2021

Between 2018 and 2021 the Romanian supervisory authority applied 68 fines, with a total amount of 721,000 Euros, which places Romania in third place in the European Economic Area for the number of GDPR fines applied.

Spain takes first place in the league table, with 351 fines applied by the supervisory authority, with a total amount of 36.7 million Euros, while Italy takes second place, with 101 fines applied by the supervisory authority, with a total amount of 89.6 million Euros.

Hungary takes fourth place, with 45 fines applied by the supervisory authority, with a total amount of 828,183 Euros, and Norway takes fifth place, with 40 fines applied by the supervisory authority, with a total amount of approximately 9 million Euros.

Although the Romanian supervisory authority has applied a large number of fines, the individual amounts were lower than those applied by the other EEA supervisory authorities.

The fines applied by the Romanian supervisory authority have targeted companies from a wide range of sectors, from large players in the finance and banking industry, to the communications industry, to e-commerce, to small and medium-sized companies in pharmaceutical field or retail.

To date, the largest fines applied by the Romanian supervisory authority have targeted large finance companies and banks and have penalized breaches of the requirement to implement appropriate technical and organizational security measures to ensure the security of personal data.

Taking into account the total number of fines applied by the EEA supervisory authorities and the total amount, the most targeted sector has been industry and commerce, which has suffered penalties totaling approximately 776 million Euros, resulting from 208 fines. Second place in the ranking is taken by the media and telecom sector, for which penalties totaling approximately 581 million Euros have been issued, resulting from 166 fines.

The most common incidents of non-compliance penalized by supervisory authorities in the EEA were the following:

- Non-compliance with general data processing principles.
- Insufficient fulfilment of information obligations.
- Insufficient legal basis for data processing.
- Insufficient compliance with data subjects' rights.
- Insufficient technical and organizational measures to ensure the security of information.

The most common incidents of non-compliance penalized by the Romanian supervisory authority were the following:

- Lack of sufficient technical and organizational measures to ensure information security.
- Lack of sufficient cooperation with the supervisory authority.
- Insufficient legal basis for data processing.

The least common incidents of non-compliance penalized by supervisory authorities in the EEA were the following: – Lack of sufficient involvement by the data protection officer. – Insufficient fulfilment of data breach notification obligations. – Inadequacy of the data processing agreement. – Lack of sufficient cooperation with the supervisory authority.	The least common incidents of non-compliance penalized by the Romanian supervisory authority were the following: – Insufficient compliance with data subjects' rights. – Non-compliance with general data processing principles. – Insufficient fulfilment of information obligations.

Contact

If you have any questions, please let us know

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

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

KPMG Legal acts in Romania through Toncescu si Asociatii SPARL

Bulgaria

Requesting Convction Certificates from Employees

The Commission for Personal Data Protection was requested to issue a statement on the matter of whether employers may rely on legitimate interest to require of newly joining employees to provide conviction certificates prior to starting employment

It is a standard practice for many employers to require starting employees to provide a conviction certificate. This is justified with the need to know of previous convictions in order to assess the suitability of the candidate to perform his/her job functions. The examples presented before the Commission for Personal Data Protection (CPDP) in the request for a statement included a case of a vacant position for a driver for which an individual convicted for motoring offences applies or a position for an IT specialist where the candidate is a convicted cybercriminal. Additional argument provided is that previous convictions may need to be known for security purposes as applying individual may have been convicted for violent crimes, thievery, etc., which may negative affect the personnel.

In its statement the CPDP outlines that as per applicable legislation, a convition certificate must be provided by the future employee only where an act of parliament or another legislative act requires evidence of good character. These are situations where a legislative act prohibits individuals convicted for certain crimes or convicted at all to occupy particular job positions, e.g. the position of a teacher cannot be occupied by an individual convicted for deliberately committing an offence.

The CPDP thefore holds that processing data contained in a conviction certificate may only be carried out on the grounds of a legal obligation, but not on the basis of a legitimate interest. Processing on the grounds of legitimate interset is considered contrary to the requirements of Article 10 of the General Data Protection Regulaton, as well.

It is further stressed on the fact that the conviction certificate in Bulgaria contains multiple details of a highly sensitive nature. By introducting stricter rules and limitations on processing data contained therein, applicable legislation is aimed at avoiding intrusion in the personal lives of data subjects, including convicts who strive to find their way back into society.

Considering the above, CPDP excludes the possibility for the legitimate interest of a company in these sitatuations to be prevailing against the interests of data subjects. The statement of the CPDP is expected to lead to abolishing the practice of requiring a conviction certificate from all future employees.

B Court Decision on Balancing Right of Free Speech and Right of Privacy

The Supreme Administrative Court quashed a decision of the first instance court formulating criteria for assessing the balance between the right to freedom of expression and information and the right to protection of personal data

The Supreme Administrative Court (SAC) adopted a decision over a case of the Commission for Persona Data Protection (CPDP) against an electronic media concerning a publication of personal data for a public figure within a journalistic article.

The SAC ruled in favor of the CPDP's rulling stating that the derogations provided in the General Data Protection Regulaton (GDPR) and the Personal Data Protection Act (PDPA) do no relieve media from honoring individual's right of privacy. A balance have to be struck between freedom of speech for journalistic expression and the right of privacy. Furthermore, data protection principles under GDPR remain applicable for the media, especially data minimization principle.

The SAC held that the media publication may include only the personal details necessary for satisfying the freedom of expression and the right of information. Including details that lead to an illegitimate intrusion in the private life of the individual shall not be allowed.

The fact that the subject of the publication is a public figure does not exclude the obligation of the media to respect the right of privacy. Furthermore, the fact that the source of some of the personal details is a public register (Property Register), does not mean the data may be published as is, as these registers' function is not journalistic expression.

The SAC decision is the first judicial act to stress on the need to strike a balance between freedom of speech for journalistic expression and the right of privacy. It shall be heavily relied upon, especially considering that back in 2019 the Constitutional Court rendered provisions of the PDPA which listed circumstances to be taken into account for said balance contrary to the Constitution of the Republic of Bulgaria.

Contact

If you have any questions, please let us know

Dilyana Dimitrova
Senior Manager
KPMG in Bulgaria OOD
T: +35929697300
E: dkdimitrova@kpmg.com

Teodor Mihalev
Senior Associate
KPMG in Bulgaria OOD
T: +35929697300
E: tmihalev@kpmg.com

Czech Republic

A

Cookies – "new" opt-in principle legislative change

The new year 2022 brings significant changes to the Czech legal regulation of cookies tracking. Since 1 January, cookies can only be collected and processed upon a prior consent of the user.

Until now, the Czech legal regulation has been unclear when it came to cookies (text files which help to identify visitors of a website and track their behavior on it) and associated consent requirement. Website operators as well as the expert community have very often interpreted the consent requirement to be based on the opt-out principle. This interpretation allowed for the cookies to be collected and processed unless the user specifically refused. In practice, the website operator informed the visitor about the processing of cookies and about the possibility to refuse it when entering the website. In case the visitor refused, he could not use all functions of the visited website.

However, this Czech regulation was not entirely in line with the EU rules, specifically with the Directive on Privacy and Electronic Communications. This Directive bases cookies tracking on the opposite, the opt-in principle. It requires website operators to obtain explicit consent from website visitors to track their activity by using cookies. Without the consent, the website operator is not allowed to collect cookies and process them.

The discrepancy and ambiguity should be eliminated by an amendment to the Czech Act on Electronic Communications, which introduced the clear opt-in principle into the Czech law. Consequently, the website operators are now facing a new obligation. To lawfully collect and process cookies they need to obtain verifiable consent from their website visitors and inform them on the scope and purpose of such processing as well as a possibility to revoke the consent.

The requirement of consent to the processing of cookies will not be fulfilled if e-shop or website operators obtain the consent using 'cookie walls', i.e. a setup that prevents access to the website or use of certain functions without consenting to cookies. The reason is that consent thus obtained (a rather common practice) cannot be considered voluntary. Similarly, the GDPR requirement that consent must be given by a specific indication of the individual's wishes shall not have been met if the box indicating the consent has already been pre-ticked by the website or e-shop. Instead, any processing of cookies based on consent obtained using the methods above will be contrary to the law.

The website operators should not take this legislative change lightly and they should update their cookies policy. It is important to stress that in the event of any dispute, the burden of proof lies with the website operator who must be able to prove that the user has given the consent to cookies processing.

B

Telemarketing and a prior consent

As of 1 January 2022, it is possible to contact the public by phone for marketing purposes only with the prior consent of the persons concerned.

Beside the collecting of cookies, the amendment to the Czech Act on Electronic Communications has also a fundamental effect on call centre operators.

The previous regulation concerning telemarketing was based on the opt-out principle. This means that the user of a particular phone number had a chance to request not to be contacted for the telemarketing purposes any longer. The prior action of the user was necessary for not be contacted by marketing callers.

Under the new rules, if the user of a particular phone number does not explicitly give consent to telemarketing, it means that they do not wish to be contacted by the call centre for marketing purposes and the call center is therefore not allowed to call them. The regulation applies to both individuals and legal persons.

If this provision is breached, entrepreneurs may be facing a penalty up to the higher of CZK 50 million and 10% of their net turnover for the last completed accounting period.

Since the new regulation is already effective, it is recommendable to have the approach to marketing calls reviewed. In view of the new regulation, we also recommend carrying out an overall review of the personal data protection policy to ensure it complies with the requirements of the amendment to the Electronic Communications Act, and those of the GDPR.

Contact

If you have any questions, please let us know

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

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

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

Greece

Data breach and unlawful data processing in the telecommunications sector

The Hellenic Data Protection Authority (HDPA) in early January 2022 issued its decision whereby it fined two companies belonging to the largest technology group of companies in Greece for violations of the GDPR and the national legislation on the protection of personal data and privacy in the electronic telecommunications sector, following a data breach concerning leakage of subscriber call data.

Following a data breach notification by one of the largest telecom operators in Greece, the HDPA investigated the circumstances under which the data breach occurred. In the context of the said investigation, the HDPA examined the lawfulness with regard to record-keeping and the security measures applied.

The initial point of origin of the incident in terms of security was the installation of malicious software on a server owned by one of the group companies. The leaked file included subscriber call data for the time period 1/9/2020 – 5/9/2020, concerning data of subscribers of the telecom operator, as well as subscribers of other operators, who, during the period in question, had electronic communication with the subscribers of the telecom operator. The compromised file included subscriber traffic and location data and was maintained by the telecom operator for two purposes: (i) To manage problems and handle malfunctions. In this case the file was maintained for three (3) months from the time the calls are made. (ii) To reach statistical conclusions for network development purposes. In this case the file included pseudonymized data (as opposed to the assertion of the company that the data were anonymized) and was maintained for twelve (12) months.

From the investigation of the incident, the HDPA concluded that the telecom operator: a) violated the principles of lawfulness of processing and transparency due to unclear and incomplete information provided to its subscribers; b) proceeded to an incomplete implementation of the data protection impact assessment and an incomplete anonymization procedure, and c) had in place inadequate security measures without designating the roles of the two companies of the group involved in the respective processing. Moreover, the other group company which owned the server that became the initial point of origin of the incident and was involved in the processing, was also found to have violated the GDPR due to inadequate security measures with regard to the infrastructure used in the context of the incident.

The above findings resulted to the imposition of heavy fines amounting to EUR 6 000 000 for the telecom operator as well as the interruption of data processing and destruction of data. The HDPA also fined the other group company/owner of the server involved in the incident with a fine amounting to EUR 3 250 000.

B

Data breach and no DPO appointment by the Ministry of Tourism

The HDPA fined the Greek Ministry of Tourism in late December 2021 for not having appointed a DPO and for not reporting a data breach which occurred in the context of the Ministry's program "Tourism for all".

In July 2020, the HDPA received a complaint from a citizen with regard to a data breach related to the operation of the platform "tourism4all" of the Greek Ministry of Tourism. In particular, upon entering his credentials in the platform in order to submit his application for the respective program, the citizen gained access to a third person's data including name, TIN, social security number, address, contact details as well as health data.

During the investigation of the data breach, the HDPA found that the Ministry of Tourism appointed a Data Protection Officer three (3) years after the entry into force of the GDPR, i.e. in July 2021 and that the website of the platform included inaccurate information on the existence of the DPO and his/her contact details.

The HDPA ruled that the assertion of the Ministry of Tourism that it did not report the data breach because i) the citizen had already informed both the HDPA and the affected data subject, without the latter taking any course of action and ii) the Ministry immediately took action to address the incident, do not substantiate an exemption from the obligation to report the data breach to the HDPA.

Moreover, the HDPA ruled that the non-existence of a contract in writing or other legal act between the Ministry of Tourism and the other public authorities/ private parties involved in the processing as Data Processors, apart from violating the respective provisions of the GDPR, it does not enable the designation of a clear procedure to handle security incidents, with clear distinction and determination of the role and liability of each party involved in the processing. Also HDPA highlighted in its decision that Data Sub-Processors which may also be involved in the processing, such as cloud providers may result in transfer of personal data outside the EU, requiring a risk assessment for the compliance of the cloud provider with the Recommendations of the EDPB of 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

As a result, the HDPA imposed a fine on the Ministry of Tourism amounting to EUR 75 000.

C

Athens Bar Association elections – Candidates' access to members data

The HDPA issued an opinion on the provision of the data of lawyers/ members of the Athens Bar Association to the candidates for the elections of the governing bodies of the Athens Bar Association.

In early November 2021, the HDPA issued an opinion on whether the provision of the lawyers/members' data to the candidates of the elections of the governing bodies of the Athens Bar Association (Association) is in compliance with the data protection legislation.

In particular, the personal data in question included: name, father's name, address, Athens Bar Association Member No., telephone number, email.

Pursuant to the HDPA, the operation of an Association also entails holding the elections of the Association. Hence, the members shall be informed on the candidates and their views in order for them to decide who to vote.

In particular, the main points addressed by the HDPA were the following:

- The candidates are third parties vis-à-vis the Association and are therefore considered to be separate data controllers;
- The capacity of being a member of the Association is not considered to be special category of data;
- The lawfulness of the data transfer may be considered as having been carried out in the public interest;
- Although the data subjects have not been informed, the purpose of the processing is linked to the initial purpose;
- The Association shall take the appropriate measures for the transfer of data;
- Each candidate shall address any right to object raised by the data subjects concerned.

D

Important updates

In order to facilitate SMEs to comply with GDPR requirements and to promote the creation of by design compliant products and services, the HDPA coordinates the "byDesign" project with duration 24 months, having started in November 2020.

Following the identification of the needs and gaps of the SMEs' compliance with the GDPR, a sample of good practice material has been assembled, which reflects recognized good practices in the major topics assessed (lawfulness and transparency; accountability; business activities entailing data processing). The next step of the project is to develop the relevant online toolkit in order to facilitate the self-assistance for the SMEs and provide them with practical information and templates on their compliance.

Contact

If you have any questions, please let us know

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

Christianna Valinaki
Lawyer/Manager
KPMG in Greece
T: +30 210 60 62 159
E: cvalinaki@kpmg.gr

South Africa

POPIA also has extraterritorial application

The extraterritorial application of the GDPR caused great consternation amongst foreign organisations, sending them to hurriedly obtain legal opinions to understand the impact of the GDPR on their businesses and to understand what the consequences would be for non-compliance. However, it seems that the extraterritorial application of South Africa's privacy law, the Protection of Personal Information Act 4 of 2013 ("POPIA"), has not received as much attention from foreign organisations. In this issue of the GLS Newsletter we explore the extraterritorial application of POPIA and explain what the consequences may be for impacted foreign organisations.

Section 3(1) of POPIA governs the application of POPIA and expressly states that the Act:

> "…applies to the processing of personal information—
>
> *a) entered in a record by or for a responsible party by making use of automated or nonautomated means: Provided that when the recorded personal information is processed by nonautomated means, it forms part of a filing system or is intended to form part thereof; and*
>
> *b) where the responsible party is—*
> *i. domiciled in the Republic: or*
> *ii. not domiciled in the Republic, but makes use of automated or nonautomated means in the Republic, unless those means are used only to forward personal information through the Republic."*

By the inclusion of Section 3(1)(b)(i), POPIA is given extra-territorial jurisdiction over foreign organisations (i.e. organisations not domiciled in South Africa). However, to apply extraterritorially:

- the information being processed must be "personal information" as defined in POPIA;
- the foreign organisation must be acting in the capacity of a responsible party (which has a similar meaning to the GDPR's 'controller');
- the personal information must be entered into a record or otherwise be intended to form part of a filing system. Importantly, this criterion will be met whether the personal information is entered into a record / filing system by the foreign organisation itself or by a third party acting on behalf of the foreign organisation; and
- if the processing of personal information occurs in South Africa (whether by automated or non-automated means). The only proviso being that POPIA would not apply where the processing is solely to forward personal information through South Africa.

Interestingly, while the GDPR explicitly applies to both foreign controllers and foreign processors, the application of POPIA appears to be limited to 'responsibility parties' (i.e. public or private bodies or any other person which, alone or in conjunction with others, determine the purpose of and means for processing personal information).

This becomes relevant as more and more companies are outsourcing business processes to offshore companies. Indeed, South Africa has become a popular choice for many foreign companies who outsource various business processes to South African service providers who are able to provide cost-effective and high-quality services. These services include, for example, call centre / contact centre services, back office support, alternative legal services, and human resource services (such as recruitment).

Having regard to the criteria set out above, in our view many of these services outsourced to South African companies would bring the foreign organisation into the ambit of POPIA as:

- the provision of these services often involve the processing of "personal information";
- the foreign organisation would likely, alone or in conjunction with others, determine the purpose of and means for processing personal information and would therefore be considered a "responsible party" in terms of POPIA;
- the personal information would typically be entered into a record or filing system by the foreign organisation itself or by the South African service provider; and
- the processing of personal information would occur in South Africa (i.e. the South African service provider would be processing personal information in South Africa).

Accordingly, in the scenario above, the foreign company would be required to comply with POPIA in respect of those processing activities.

A similar situation would likely arise where a foreign company makes use of cloud services hosted in South Africa or where a multinational transfers personal information to a South African group company for processing.

Responsible parties who are non-compliant with POPIA can face:

- enforcement notices which requires the responsible party to take specified steps or to refrain from taking such steps;
- enforcement notices which requires the responsible party to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice;
- civil action being instituted by a data subject which may result in the award of compensation being payable for patrimonial and non-patrimonial loss suffered by the data subject; aggravated damages; interest and costs of the lawsuit;
- conviction of an offence (for example where the responsible party fails to comply with an enforcement notice) punishable by a fine and/or imprisonment for a period not exceeding 10 years;
- the issuance of an infringement notice in terms of which the infringer may be issued an administrative fine not exceeding ZAR 10 million.

As POPIA has only recently become effective (on 1 July 2020), we are yet to see how the Information Regulator exercises these enforcement powers particularly against non-compliant responsible parties that are not domiciled in South Africa. However, we urge foreign organisations with touchpoints in South Africa to assess whether POPIA applies to its processing activities and, if so, what actions should be taken to ensure compliance with its obligations in terms of POPIA.

Contact

If you have any questions, please let us know

Beulah Simpson
Senior Legal Manager
KPMG in South Africa
T: +27 (0) 60 602 3066
E: Beulah.Simpson@kpmg.co.za

Farah Jakoet
Legal Manager
KPMG in South Africa
T: ++27 (0) 66 474 2780
E: Farah.Jakoet@kpmg.co.za

Meelan Manga
Legal Consultant
KPMG in South Africa
T: +27 (0)71 492 6340
E: Meelan.Manga@kpmg.co.za

Nigeria

Telemedicine in Nigeria: Data Protection Considerations

Introduction

In March 2020, the World Health Organization (WHO) declared COVID-19 a pandemic, pointing to the several cases of the coronavirus in over 110 countries and territories around the world and the sustained risk of further global spread of the virus. The declaration was necessitated by the spread of a disease, rather than the severity of the illness it causes. Several countries had at this time, initiated lockdown procedures to prevent a further spread of the disease because as the total number of infections rose, so too did the number of cases that spread from person-to-person within communities around the world. Hospitals began to seek other avenues (mostly virtual) separate from in-person consultation, which would provide the much-needed healthcare as well as ensure the safety of all health workers and patients needing healthcare for non-critical ailments, by averting further contact with such high-risk patients.

Telemedicine and its application in Nigeria.

One of these avenues which was actively utilized is Telemedicine. Leveraging Telemedicine to combat the disease worldwide became crucial. The WHO has adopted the following as the definition of Telemedicine- "delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities".

Telemedicine seeks to improve a patient's health by a permitting two-way, real time interactive communication between the patient, and the physician or medical practitioner at the distant site. It involves the use of telecommunication technologies to prevent and treat illness and promote the health of individuals and populations. The electronic communication means the use of interactive telecommunications equipment that includes, at a minimum, audio and video equipment. Also, at the heart of the application of Telemedicine in Nigeria is the type of personal data gathered while providing medical services via these electronic platforms. Such personal data may include but is not limited to names, phone numbers, home and email addresses, date of birth, sex, medical history, of the patient.

NDPR and Data Protection Considerations

The National Information Technology Development Agency (NITDA) is statutorily mandated by the NITDA Act of 2007 to develop regulations for electronic governance and monitoring of the use of information technology and electronic data. Conscious of the concerns around privacy and protection of Personal Data and the grave consequences of leaving Personal Data processing unregulated, NITDA issued the Nigeria Data Protection Regulation (NDPR) in 2019. The objectives of the NDPR are as follows:

- to safeguard the rights of natural persons to data privacy;

- to foster safe conduct for transactions involving the exchange of Personal Data;
- to prevent manipulation of Personal Data; and
- to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a sound data protection regulation.

The NDPR applies to all processing and storage of Personal Data conducted in respect of Nigerian citizens and residents.

At the core of Data Protection are the privacy principles which include but are not limited to the following:

- ***Data Security:*** where data controllers and processors are expected to implement security measures (including firewalls, data encryption technologies, etc.) to protect data from theft, cyber-attack, manipulations, environmental hazards, etc.
- ***Lawful Processing:*** where at least, one of the following applies i.e. consent has been given, processing is necessary for the performance of a contract, compliance with a legal obligation, protection of the vital interests of the Data Subject or any public interests.
- ***Data Integrity and Storage Limitation:*** where personal data is adequate, accurate and stored only for the period within which it is reasonably needed.

The success of Telemedicine could be undermined if privacy and security risks are not addressed. Considering the above, Data Controllers/Health Practitioners are required to take note of the following with respect to Telemedicine:

a. One core issue is the matter of the rights and confidentiality of patients while using Telemedicine. There are no formal Telemedicine protocols and procedures yet in effect in Nigeria. Several patients and health-workers are unaware of the quality of practice and how confidentiality should be protected. For example, although the NDPR is generic to personal data in whatsoever sphere/sector in Nigeria, the specificity of privacy rules for medical data in other climes is lacking in Nigeria.

b. Liability of a party with respect to data collection, transmission, storage, deletion, back-up/recovery, etc, where the managing of the technology software/platform is outsourced to another entity or the platform is owned by another entity and leased by the health service provider.

Other Jurisdictions and the regulation of personal data from Telemedicine

United States of America.

The Health Insurance Portability and Accountability Act (HIPAA) is a legislation enacted in the USA which directs the U.S. Department of Health and Human Services (HHS) to establish national standards for processing electronic healthcare transactions. The HIPAA has set out privacy and security rules for safeguarding medical information, and which require that the information gathered through a telemedicine service is encrypted alongside the network connections being utilized. Additionally, when contacting patients, one is required to ensure that the patients are messaged through a secure connection. Also, before recording and storing video calls, the permission of the patient is required. It also requires healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS.

Under the HIPAA, where there is a healthcare data breach the penalties range from as low as $100 per violation to $1.5 million for repeat violations, depending on the severity of the infraction.

Closely linked to the HIPAA is the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, where the US Congress extended the HIPAA to "business associates," entities that "create, receive, maintain, or transmit" identifiable health information to perform a function or service "on behalf of" a covered entity. Relevant questions covered by the HITECH include the following: Who provides the technology to the patient (for example, is it a direct-to-patient transaction, or is the technology provided by the doctor)? Who is responsible for the day-to-day operation of the technology (an indication of who is ultimately responsible)? And who controls the information generated by the technology?

Nigeria- Data Protection (DP) Framework (NDPR & Proposed DP Bill)

The current DP framework in Nigeria does not specifically provide for the security of health-related personal data and the entire cycle of data collection, processing, retention and finally, ultimate deletion, given the unique nature of health-related personal data. Relatedly, the NDPR does not mention data retention and this is an issue to be considered, as the personal data of an individual who passes on or is no more a patient to the medical facility hosting the platform or providing the health service, is seemingly not regulated by any contract or legislation.

Furthermore, the liability of a third party (typically where based in a foreign country) who hosts the Telemedicine platform may not be established. This is because the transfer of such data to a foreign country should have been done under the supervision of the Attorney General of the Federation, where the decision is that the foreign country ensures an adequate level of protection. However, where this is not the case, the ability of the regulatory agencies to determine that there has been a breach and impose the appropriate penalties on the liable party, may be difficult. Moreover, the penalties provided by the NDPR may not be stiff enough to ensure compliance with the regulation.

Conclusion/Recommendation

A Telemedicine consultation requires exchanging patient information; thus, it must be done in a manner that the privacy and safety of such information are protected. Privately gathering the information means conducting the consultation in such a way that no one else who is not supposed to be part of the consultation can see the report or hear the conversation. Sending the information safely ensures that only those who are engaging directly in the patient's treatment will have the ability to access it. It is during this process that privacy measures come into play and the question is whether the NDPR is sufficient to back up those privacy principles. Concerns about the privacy and security of Telemedicine systems may adversely affect people's trust in Telemedicine and threaten the ability of these systems to improve the accessibility, quality, and effectiveness of health care. More comprehensive standards and regulations may be needed to ensure stronger privacy and security protections in Nigeria.

Contact

If you have any questions, please let us know

Beulah Simpson
Senior Legal Manager
KPMG in South Africa
T: +27 (0) 60 602 3066
E: Beulah.Simpson@kpmg.co.za

Farah Jakoet
Legal Manager
KPMG in South Africa
T: ++27 (0) 66 474 2780
E: Farah.Jakoet@kpmg.co.za

kpmg.com/socialmedia