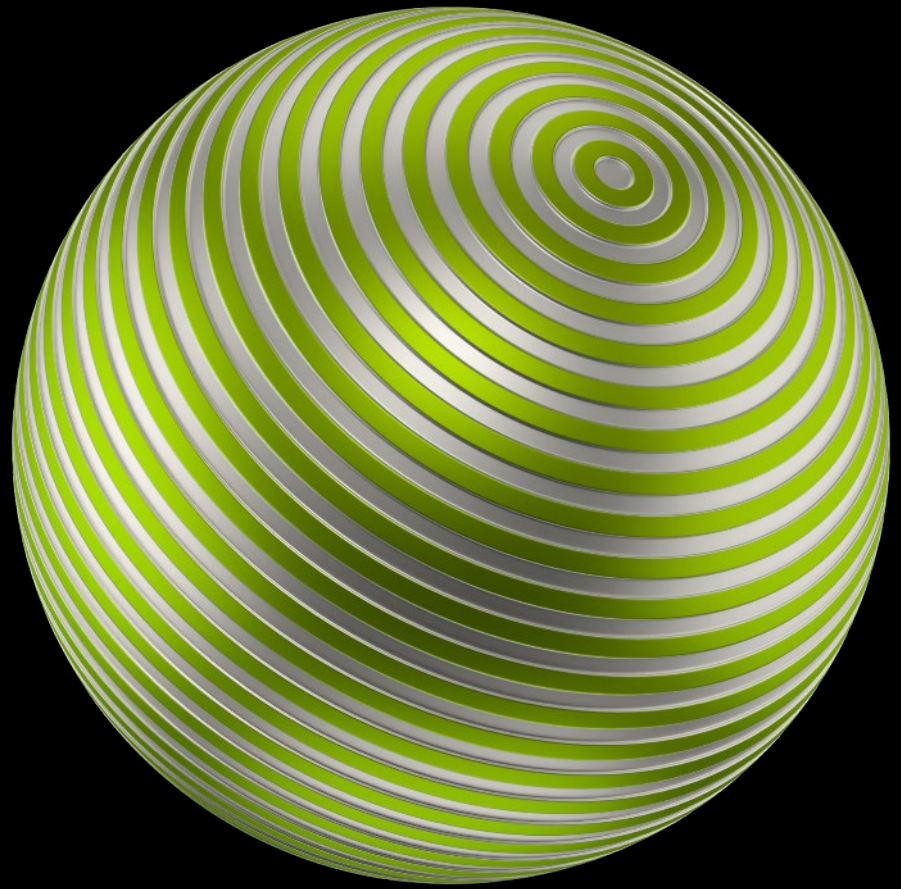
Deloitte.
Legal



Recent updates and upcoming developments

Cross jurisdictional data protection overview

December 2022

MAKING AN IMPACT THAT MATTERS since 1845

Index

Introduction

Deloitte Legal addresses your challenges with comprehensive thinking, powered by experience and insights drawn from diverse business disciplines, industries, and global perspectives.

We bring together legal advice, strategy, and technology to develop innovative solutions, create value for you and your business, and transform the way in which legal services are delivered and consumed. The future of law is here, today.

Experience the future of law, *today.*

Experience the future of law, today

An introduction to Deloitte Legal

Deloitte Legal is

more than

2,500

legal professionals

operating in

75+

jurisdictions

collaborating seamlessly

across borders and with other Deloitte business lines

We apply perspective to deliver value

Deloitte's cross-disciplinary approach enables us to provide globally integrated services that are:

Consistent
with your enterprise-wide vision

Technology-enabled
for improved collaboration and transparency

Tailored
to your business units and geographies

Sensitized
to your regulatory requirements

Deloitte Legal practice areas

We are organized into three intersecting market offerings, enabling us to serve our clients when, how, and where we can help them achieve their visions.

Jurisdictional advisory

Legal function strategy, technology & process automation

Outsourced legal obligations and legal managed services

Perspective that is global and grounded

Legal services traditionally provide specialist expertise with a grounded perspective. Deloitte Legal's broader, global perspective, informed by its multi-disciplinary approach and extensive industry and technological expertise, enables fully-integrated smart solutions to be developed that expand customer expectations, redefining what is possible. Global capabilities that are locally grounded can help you address an increasingly complex world. One relationship provides endless connections.

Overview

A complex framework, a cross jurisdictional approach

In today's digital economy, a strategic data governance is crucial for businesses of all sizes and operating in any industry. The enter into force of the General Data Protection Regulation (GDPR) in 2018 provided economical operators a uniform legal framework that helped in structuring procedures, documents, contractual relationships, etc. on common basis.

On one side, the GDPR contains principles and provisions which leave a wide margin of discretion concerning their respect.

On the other side, data controllers and processors are required to, in addition to the GDPR, respect all national laws and the guidelines and decisions of the supervisory authorities.

Moreover, after four years of effectiveness of the GDPR, thanks to the interpretation given to the privacy and data protection laws by courts, authorities and practitioners, some best practices have been established.

In order to comply with the applicable complex legal framework and to achieve in the organizations an effective data management, an integrated approach is therefore fundamental and Deloitte Legal is the ideal partner for that.

This document consolidates an overview across 10 jurisdictions on:

- ✓ The most relevant data protection laws, regulations, guidelines, decisions and sanctions of the last months; and
- ✓ Some upcoming developments in the data protection field foreseen by Deloitte Legal teams over the next months.

Past

Most relevant data protection updates of the last months

Future

Expected developments concerning data protection that can be foreseen may be coming up in the next months

National updates and developments

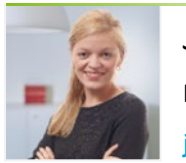
Belgium

Contacts

Matthias Vierstraete

Director

mvierstraete@deloitte.com



Julie Van Com

Managing Associate

jvancom@deloitte.com

What are the most relevant **data protection updates of the last months**?

The past year, no noteworthy updates to legislation have taken place regarding data protection in Belgium. However, several interesting **decisions and sanctions** have been adopted by the **Belgian Data Protection Authority** (BDPA), relating to several aspects:

Enforcement of transparency and consent obligations

In its Decision 21/2022: IAB Europe deployed an application titled "Transparency and Consent Framework" (TCF). This TCF is a popular mechanism that facilitates the management of user preferences for online personalized ads and plays a key role in so-called "Real-Time Bidding" (RTB) process, an automated online auction of user profiles for the sale and purchase of advertising space on the internet. Following several complaints, and an inspection by the BDPA, the BDPA, identified a series of breaches of the GDPR by a European advertising body (*inter alia* with regards to user transparency and information, accountability, security, data protection by design and by default, no records of processing activities, no data protection impact assessment (DPIA) carried out, no data protection officer (DPO), etc.). As a result of these infringements, the Dispute Resolution Chamber of the GBA imposed serious penalties, particularly because the TCF can cause a large group of citizens to lose control over their personal information. The BDPA has imposed an administrative fine of €250,000 on the advertising body. It also ordered the company to take a series of corrective measures and bring the current version of the TCF into line with the GDPR.

Cookie-related decisions

The BDPA is currently conducting a broad investigation into the use of cookies on the most popular Belgian press websites. The Inspection Service of the BDPA has already examined 20 different websites. Within this investigation, not all targets are fined at once or with one single decision. The Litigation Chamber is currently examining other files in this context. Recently, two companies have already been fined in two separate decisions:

Decision 85/2022: A media company was fined €50,000 for not following the relevant cookie-legislation. Several infringements under the GDPR were identified. For example: regarding the 'prior consent', approximately 60 cookies (no strictly necessary cookies) had been placed on the user's device by websites before they had given their consent. The company was also found to be negligent in providing information about cookies to the users of its websites etc.

Decision 103/2022: The second fine concerning this broad investigation, amounting up to €50,000, was imposed on another media company, for not having its cookie-policy and usage in line with the GDPR. There was no prior consent obtained for several non-necessary cookies, the cookie policy was unclear and incomplete, pre-ticked boxes were used, etc.

What are the most relevant **data protection updates of the last months**?

Recently, no noteworthy updates to legislation have taken place. However, several interesting **decisions and sanctions** have been adopted by the **Belgian Data Protection Authority** (BDPA), relating to several aspects:

COVID-19 and other health-related decisions:

In decision 47/2022 the BDPA fined an airport €100,000 for their use of thermal imaging cameras as part of measures to control COVID-19. The airport used thermal imaging cameras to filter out people with body temperatures above 38 degrees. Those filtered out were then required to answer questions about possible coronavirus symptoms. In its decision, great importance was attached to the principles of lawfulness and necessity of the processing activities, to the absence of a Data Protection Impact Assessment, and to the fact that data subjects were not sufficiently informed of their sensitive health data being processed.

In its decision 48/2022 the BDPA fined a commercial Belgian airport €200,000. The exact same reasons and reasoning as mentioned above was followed in this case.

In its **decision 127/2022** the BDPA fined a medical laboratory €20,000 for analyzing sensitive health data while insufficient technical and organizational measures were in place to ensure information security (no HTTPS protocol was used and the encryption protocol used showed vulnerabilities). Additionally, the laboratory had failed to conduct a data protection impact assessment before the start of the processing activity even though physicians were processing special categories of data on a large scale (personal data concerning health of patients). Finally, the BDPA found that the laboratory had not published a privacy statement on its website to inform patients on the processing of their personal data in accordance with Articles 12,13 and 14 of the GDPR.

We can conclude from the previously mentioned cases that an enhanced focus is placed by the BDPA on technological developments such as a Transparency and Consent Framework or cookies, and that even in times of urgency, such as a global pandemic, data protection cannot be that easily pushed aside.

What are the most relevant **data protection developments foreseen upcoming in the next months**?

The BDPA recently published its **2022 Management Plan,** in which it sets out some of its key focus points for the year.

Firstly, the Inspection Service (the body carrying out the investigations) will try to put an enhanced focus on processing activities in the context of **direct marketing**, on **sector-wide cookie investigations** and on **large-scale processing of sensitive data** within the life science and health care sector (e.g., hospitals).

Secondly, another interesting point put forward in this management plan, is the fact that the Litigation Chamber, the body responsible for handling the proceedings and imposing fines or sanctions, intends to publish a **sanctions policy**, outlining the reasoning behind sanctions and developing a **"toolbox"** to make the fines more objective and universal. Moreover, this plan states a key focus will be the effective follow-up of sanctions, as well as keeping the proceedings' duration within a reasonable timeframe of three months (except in complex cases).

A new Belgian **Act on data retention** has been published in the Belgian Official Gazette on 8 August 2022, as the previous version of this Act was annulled by the Belgian Constitutional Court over reasons of privacy. The Act governs the storage of telephony metadata by telecom operators, and allows the Belgian courts and other public authorities, such as tax authorities, to retrieve that data if deemed necessary. The aim is to strike the right balance between privacy and data protection on the one hand and accessibility for the courts and other public authorities on the other to conduct investigations. The police will for example have the right to certain data such as the name, first name, national register number, IP address and phone number but will not have access to the content of the phone call.

The Council of Ministers has approved a preliminary draft law that responds to the recommendations of an evaluation report of the **"Act of 3 December 2017 establishing the BDPA".** This evaluation recommended to strengthen the pragmatic approach and sectoral expertise of the BPDA by, among other things, enhancing cooperation with other authorities. Moreover, the report recommended to strengthen the independence and the functioning of the Belgian Data Protection Authority, by, among other things, granting the GBA more discretion to lay down its internal functioning, organization and rules of procedure and by stipulating that the BPDA is the only competent authority to carry out the tasks and mandates concerning the supervision of compliance with the GDPR. These recommendations were adopted in this newly approved preliminary draft law.

Following this preliminary draft law however, the BDPA has issued its own draft advice, as it is of the opinion that this preliminary draft law seriously jeopardizes both the efficient functioning and the independence of the authority, even though it aims to strengthen it. This jeopardization is said to occur because the preliminary draft provides for parliamentary interference in the setting of priorities and the internal organization of the BDPA.

France

Contacts

Hervé Gabadou

Partner

hgabadou@avocats.deloitte.fr

Tony Baudot

Senior Manager

tbaudot@avocats.deloitte.fr

What are the most relevant data protection updates of the last months?

The French National Commission for Information Technology and Civil Liberties (CNIL) wanted to control three main themes in 2022 in France:

Commercial prospecting

Unsolicited commercial canvassing is a recurring subject of complaints to the CNIL. In February 2022, the CNIL published a new commercial management reference framework, which provides a framework for commercial canvassing. It's accompanied by several pieces of information on the CNIL website to guide those involved in the process of compliance.
The CNIL imposed three major sanctions, notably for having carried out commercial prospecting without the consent of the persons concerned and for not having respected the rights of customers and prospects (the right to information and the right of opposition).

Surveillance tools in the workplace

Since telecommuting became mandatory, the CNIL has wanted to address the issue of work-related surveillance tools. It has adopted a series of rules and good practices to be respected in order to ensure a fair balance between privacy at work and legitimate control of workers' activities.

The use of cloud computing

The use of the cloud entails certain risks for the protection of personal data, due to massive transfers of data outside the EU to countries that do not provide an adequate level of protection or data breaches in the event of incorrect configuration. However, the CNIL has not adopted any recent specific provisions on this subject.

What are the most relevant **data protection updates of the last months**?

Data protection laws and regulations, guidelines

The CNIL has not published any guidelines during 2022 and no data protection laws have been passed.

However, it has adopted several important measures to assist with GDPR compliance:

Health sector

- ✓ A draft submitted for public consultation of a reference framework relating to the processing of personal data implemented by the laboratory holding the exploitation rights of a medicinal product benefiting from a compassionate access authorization;
- ✓ A draft submitted for public consultation of a reference framework relating to the processing of personal data implemented by the laboratory holder of the exploitation rights of a medicinal product benefiting from an authorization for early access;
- ✓ A reference framework relating to the processing of personal data intended for the management of pharmacies; and
- ✓ A compliance checklist relating to the processing of personal data implemented for the purpose of creating data warehouses in the health sector.

Commercial relations and payments

- ✓ A repository on the processing of personal data implemented for the purpose of managing commercial activities (prospects, customers);
- ✓ A repository on the processing of personal data for the purpose of managing unpaid bills in a commercial transaction; and
- ✓ A white paper on data and payment methods.

What are the most relevant data protection updates of the last months?

Recent cases

29 October 2022. The CNIL fined a public enterprise of an industrial and commercial nature that operates part of the public transport system in Paris and its suburbs. The union organization filed a complaint with the data protection authority, claiming that an evaluation file for their employees contained a number of categories of personal data that would make it illegal and even discriminatory. After an inspection, the CNIL established that the principles of data minimization and responsibility were not respected, that the data was not kept for a sufficient period of time and that there was a lack of data security.

31 October 2022. The CNIL heavily sanctioned two large global technology companies to the tune of €60 million and €150 million due to their cookie refusal methods. In both cases, neither allow both the refusal and acceptance of cookies.

31 May 2022. The CNIL gave notice to 22 local authorities to find a DPO within four months. This decision reflects the interest of the data protection authority in bringing public sector actors into compliance. Since then, 18 local authorities have found a DPO, while penalties could be imposed on the others.

13 September 2022. The CNIL imposed a penalty on a public interest grouping that publishes legal and official information on companies. It operates a public service delegation provided for by law. The grouping was been sanctioned for failing to comply with several GDPR obligations regarding retention periods and security of personal data.

What are the most relevant **data protection developments foreseen upcoming in the next months**?

There is little communication on the CNIL's upcoming projects. However, the CNIL has unveiled its new 2022-2024 strategic plan around three priorities for a trusted digital society:

- ✓ Promote the control and respect of the rights of individuals;
- ✓ Promote the GDPR as a confidence-building for data controllers; and
- ✓ Prioritize targeted regulatory actions on topics of high privacy concern (augmented cameras and their uses, data transfers in cloud computing, personal data collection in smartphone applications).

The CNIL also submitted for public consultation a draft recommendation on the technical and organizational measures to be applied when organizations use application programming interfaces (APIs) to share personal data (until 1 November 2022).

Finally, due to the signature of the executive order by Joe Biden on the application of a new text framing the transfers of personal data between the European Union and the United States, the CNIL is expected to give its opinion on the adequacy of the level of data protection provided by this text.

Germany

Contacts

Klaus Brisch

Partner

Kbrisch@deloitte.de

Marco Mueller-ter Jung

Director

mmueller-terjung@deloitte.de

What are the most relevant data protection updates of the last months?

Data protection laws and regulations:

Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)

On 1 December 2021, the new German Telecommunications-Telemedia Data Protection Act (abbreviated in German to TTDSG) came into force. The Telemedia Act (TMG) and Telecommunications Act (TKG) were adapted and modernized (accordingly). Adjustments that were necessary due to the EU General Data Protection Regulation (GDPR) and the more extensive, directive-compliant implementation of the ePrivacy EU-Directive were also implemented in the TTDSG. Overall, the TTDSG can be seen as an interim step on the way towards the EU ePrivacy Regulation, which is still in the legislative process. The law is aimed at telecommunications service providers and providers of a website or app. For companies that are not telecommunication service providers, the impact of the TTDSG is not intense, but nevertheless present. Most relevant are the regulations for the use of cookies. For these, the consent of the end user is generally required according to the GDPR, unless they are so-called "strictly necessary" cookies or the provision of a telemedia service expressly requested by the user.

The reform of the law of obligations

This has such far-reaching significance that it may also have an impact on data protection law. With the "Act on the Implementation of the Directive on Certain Aspects of Contract Law relating to the Provision of Digital Content and Digital Services" and the "Act on the Regulation of the Sale of Goods with Digital Elements and Other Aspects of the Contract of Sale", which entered into force on 1 January 2022, as well as the "Act on the Amendment of the Civil Code (...) in Implementation of the EU Directive on Better Enforcement and Modernization of Union Consumer Protection Rules (...)", which followed on 28 May 2022, the law of obligations is once again being revised. This reform is of great importance for consumers as well as for business owners. This is especially the case when an entrepreneur is engaged in B2C business with digital products.

What are the most relevant data protection updates of the last months?

Regulations, guidelines, decisions and sanctions (1/3):

Data Protection Conference ("DSK"):

24 November 2021: Decision on the possibility of not applying technical and organizational measures pursuant to Art. 32 GDPR at the express request of data subjects. Technical and organizational measures (TOM) are based on objective legal obligations, which are not at the disposition of the parties involved. Reliance on TOM is not permissible.

20 December 2021: FAQ on the processing of employee data in the context of the COVID-19 pandemic.

18 February 2022: Guidance from the supervisory authorities on the processing of personal data for the purposes of direct marketing under the General Data Protection Regulation (GDPR). The guideline covers the following issues: information requirements, consent, special situations and the relation between the GDPR and direct marketing.

13 April 2022: On the processing of personal data in connection with the facility-based mandatory vaccination program .

The Federal Commissioner for Data Protection and Information Work:

Guidance on measures to protect personal data transmitted by email. The guidance indicates the requirements to be met by the procedures for sending and receiving email messages by controllers, their processors and public email service providers in transit.

What are the most relevant **data protection updates of the last months**?

Regulations, guidelines, decisions and sanctions (2/3):

States Supervisory Authority:

Baden-Württemberg

- ✓ Video conferencing systems - Guidelines for practical use
- ✓ FAQ on the delimitation of responsibilities and the concept of commissioned processing

Bremen

On 3 March 2022, the data protection authority of the Free Hanseatic City of Bremen imposed a fine of €1,900,000 on a real estate company for processing data of prospective tenants without a legal basis under data protection law. More than 9,500 pieces of data of prospective tenants were processed unlawfully.

Hamburg

The Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) imposed a fine of €901,389 on an energy company for not sufficiently informing customers about a special form of data matching. Around 500,000 people were affected.

What are the most relevant **data protection updates of the last months**?

Regulations, guidelines, decisions and sanctions (3/3):

Niedersachsen

- ✓ Data protection for local MPs Guidelines
- ✓ FAQ on the Telekommunikations-Telemediendatenschutz-Gesetz (TTDSG)
- ✓ The State Commissioner for Data Protection (LfD) of Niedersachsen had imposed a penalty of €1.1 million on an automotive manufacturer pursuant to Art. 83 of the General Data Protection Regulation (DS-GVO). This was due to data protection violations in connection with the use of a service provider during research drives for a driving assistance system to avoid traffic accidents. The company cooperated fully with the LfD Lower Saxony and accepted the fine notice.
- ✓ On 28 July 2022, the Data Protection Commissioner of Lower Saxony (LfD Niedersachsen) imposed a fine of €900,000 on a credit institution for data protection violations in the context of advertising measures. The fined credit institution analyzed the behavior of app users, the use of statement printers and the volume of transfers made in online banking and compared this data with usage data of the offer in branches. In the course of this, the credit institution worked together with a service provider and a credit agency. With this evaluation, the credit institution intended to identify and specifically address digitally affine customers.

Nordrhein-Westfalen

- ✓ Guidelines on data protection in the association

Sachsen-Anhalt

- ✓ Guidelines to data protection in small and medium-sized enterprises

What are the most relevant data protection developments foreseen upcoming in the next months?

The transposition of the whistleblowing Directive EU 2019/1937 into national law

Germany has not yet adopted the national law implementing the Directive EU 2019/1937 on the protection of whistleblowers. The deadline for transposing the EU Whistleblower Directive into national German law has been passed. On 13 April 2022, the Federal Ministry of Justice has now presented its draft bill for a Whistleblower Protection Act. The final implementation remains to be done.

Greece

Contacts

Apostolos Vorras

Partner

avorras@kbvl.gr

Christina Varytimidou

Associate

cvarytimidou@kbvl.gr

What are the most relevant **data protection updates**?

Recent guidelines

Guidelines 1/2021 on the application of the rules on personal data protection in the context of teleworking: These guidelines inter alia further clarified that continuous surveillance of the employees' screens is disproportionate, while after the end of their working day remote employees have the right to disconnect from the software and applications used during their working hours. The guidelines also specified the technical and organizational measures that must be in place to avoid spyware and to implement a BYOD (bring your own device) policy.

Recent actions

In May 2022 the HDPA announced it has so far carried out 30 audits of various websites that use cookies. In its announcement the HDPA further urged controllers to comply with its 1/2020 Guidelines, while it highlighted that the color, size and font of the buttons must be identical for all choices to ensure the user is not influenced by design choices. In addition, the user should be able, with the same number of actions ("clicks") and from the same level, to either accept the use of cookies or reject it per each category separately.

Recent opinions/recommendations

On July 2022, the Hellenic Data Protection Authority (HDPA) announced its recommendation on layered information in online environments. To ensure the information provided to data subjects under Articles 13-14 of the GDPR is concise, transparent, intelligible and written in clear and plain language, the HDPA urged data controllers to stop using extended privacy notices on pdf formats and to consider whether the privacy notice is equally accessible from a smartphone or other smaller size screen.

What are the most relevant **data protection updates**?

Recent cases

35/2022 : Following similar decisions by the CNIL, ICO and Il Garante, Greece imposed the biggest fine yet (€20 million) to a facial recognition software company after receiving a complaint by a local human rights advocacy group and one data subject. The HDPA found numerous violations of the transparency and lawfulness principles and banned the software company from processing personal data of people residing in Greece, while it also ordered it to delete all personal data concerning people residing in Greece it has so far unlawfully collected.

4/2022 : HDPA fined a group of mobile telecoms companies €9.25 million (the second biggest fine) after an investigation by the HDPA on a major data breach that occurred in 2020 due to a cyberattack on the group's information systems. The breach was promptly notified to the HDPA , but more than 10 million subscribers were affected.

Cases 19/2022, 23/2022 and 27/2022: The HDPA imposed numerous fines for breaching the right of access of data subjects. The loss of two medical certificates, thus the inability to fulfill the data subjects' right of access request led to a €9,000 fine to the Social Protection Centre, while the failure to respond to the data subject's request to receive a copy of the CCTV recording led to a fine of €2,000.

6/2022: The HDPA fined a bank €10,000 for disclosing personal data to a third party via sending Winbank alerts to the wrong email receiver. The HDPA warned the bank of the inadequacy of the technical measures in place that validate email addresses and found it to be in breach of Articless 5(1), 33-34 of the GDPR.

What are the most relevant **data protection developments foreseen**?

The newly voted Law Nr. 4961/2022 on 'Emerging information and communication technologies, strengthening digital governance and other provisions:

The law on 'Emerging information and communication technologies, strengthening digital governance and other provisions has been published since 27 July 2022 in the Official Gazette (FEK). The recently adopted legislation sets outs the requirements for deploying various types of technologies like artificial intelligence (AI), the Internet of Things, and Blockchain, while it also contains cybersecurity provisions. In particular:

- ✓ The second chapter of this legislation mostly sets out rules on the use of AI systems, by imposing obligations to both private and public sector (for the public sector more obligations are imposed, like algorithmic impact assessment and registration of all AI systems that will be deployed by public bodies). A steering committee on AI, an oversight committee for the National Strategy for the Development of Artificial Intelligence, as well as an Artificial Intelligence Observatory are also established. The provisions of this chapter will enter into force on 1 January 2023.

- ✓ As far as cybersecurity is concerned, the General Directorate for Cybersecurity of the General Secretariat for Telecommunications and Postal Services of the Ministry Digital Governance becomes the national cybersecurity certification authority under Article 58 of the Regulation EU/2019/881 and is assigned with the tasks under Articles 56-63 of the abovementioned regulation. A definition of what constitutes critical digital infrastructure is also included in the relevant chapter.

- ✓ Part B of the legislation focuses on setting out rules on the usage of emerging technologies like Internet of Things, unmanned aerial systems (UAS) for the provision of postal services, distributed ledger technologies (blockchain) and 3D printing. Especially in the context of 3D printing the liability allocation is clarified under the proposed Article 57.

Amendments to the national data protection law

A need to amend certain provisions of Law Number 4624/2019 that supplements the GDPR has already been identified, potentially directly affecting the implementation of the GDPR. However, this is still under discussion, and therefore no specific information on the amendments is feasible for now.

The transposition of the whistleblowing Directive EU 2019/1937 into national law

Greece has not yet adopted the national law implementing the Directive EU 2019/1937 on the protection of whistleblowers; the relevant legislation is foreseen to be adopted soon, specifying certain data protection issues during the reporting procedure.

Italy

Contacts

Ida Palombella
Partner
ipalombella@deloitte.it

Pietro Boccaccini
Director
pboccaccini@deloitte.it

What are the most relevant data protection updates of the last months?

Guidelines on the use of cookies and other tracking tools

On 10 June 2021, the Italian Supervisory Authority (the Garante) approved its new guidelines on the use of cookies and other tracking tools, that became effective on 9 January 2022. With such guidelines, the Garante has clarified some relevant aspects, such as that: (i) under no circumstances it is permitted to rely on the controller's legitimate interest to justify the use of cookies or other tracking tools; (ii) the mere scrolling down of the page bar is in itself unsuitable for the controller to obtain genuine consent; and (iii) a cookie wall may not be deemed to be in line with the legislation in force. Furthermore, the Garante listed mandatory elements and features of the cookie pop-up banner and of the cookie policy. Among such, the Garante recommended that: (i) the banner shall contain a warning that by closing the banner (for example by the use of an "X") the default settings are left unchanged and, therefore, browsing can continue without cookies or other tracking tools other than technical ones; and (ii) the banner shall contain a link to an additional dedicated area where the user can select the cookies that the user consents to install, and where the user can either consent or refuse to the use of all cookies with ad hoc buttons having the same design/color.

Extension of "*registro delle opposizioni*" (Do Not Call Registry) also to mobile phones

In March 2022, the Presidential Decree No 26/2022 entered into force, providing also the possibility to register mobile phone numbers into a specific objection list, named "registro delle opposizioni" (Do Not Call Registry), to object to receiving marketing and promotional calls; such registration has the effect of withdrawing any consent provided before the registration. From the end of July 2022, the renewed regime has become fully operational.

Sanction against a well-known global online transportation network company

In March 2022, the Garante, following the notification of a data breach, issued a sanction against two foreign companies of the online transportation network, since it found that the two companies should have qualified as joint data controllers since they had: (i) a common database; and (ii) the same policies, security measures and privacy notice with a single contact for the exercise of the data subjects' rights.

Sanctions against Italian media and telecoms companies for the use of Google Analytics

The Garante found that a website transferring users' personal data to the United States (US), using Google Analytics, without appropriate and effective safeguards to ensure an adequate level of protection is in breach of the data protection law. In determining that the processing was unlawful, the authority reiterated that an IP address is a personal data and would not be anonymized even if it was truncated, given Google's capabilities to enrich such data through additional information it holds.

What are the most relevant data protection updates of the last months?

Sanction against a university concerning data transfers

In September 2021, the Garante issued a decision against an Italian university, which used a software - provided by a company established in the US - in order to identify the students and/or to verify their correct behavior during the exams. In particular, (i) the privacy notice did not contain all necessary information under Article 13 of the GDPR, including the indication of data transfer to the US and the appropriate safeguards, the retention periods, etc.; (ii) the university did not carry out a transfer impact assessment (TIA) and it did not identify and adopt adequate supplementary measures; and (iii) the DPIA performed by the university was not conducted properly, without a timely assessment of the necessity and proportionality of the processing in relation to the purpose and of the risks for the rights and freedoms of data subjects.

Sanction against a media and telecommunications company concerning wild marketing

In September 2021, the Garante issued a fine against the Italian entity of a global media and telecommunications group concerning “wild telemarketing”. The main issues ascertained were: (i) making promotional calls without privacy notice or consent; (ii) using unverified lists acquired from other companies; and (iii) non-recording objections to the processing. In order to properly carry out telemarketing activities, the group, at the beginning of the phone call, should have provided data subjects with its own privacy notice, explaining also the origin of the data, and - only after obtaining consent - it could have proceeded with the commercial proposal. In addition, the Garante highlighted that the group should have checked - before carrying out any operation - its blacklists in order to verify that the data subjects had not expressed their right to objection to receiving advertising calls related to its own products.

Sanction against a well-known facial recognition company concerning biometrics

In February 2022, the Garante imposed to the company a fine of €20 million as well as an order to erase the data of individuals in Italy and to cease any further collection and processing of personal data. The authority found that the abovementioned company was unlawfully processing personal data, including biometric data, by the use of web data scraping for facial recognition purposes. In particular, the Garante determined that such processing was carried out: (i) without adequately informing the data subjects; and (ii) without a valid legal basis for the processing (since the controller could not rely on a legitimate interest and no legal ground was applicable to the processing of biometric data). Moreover, the company failed to nominate a representative in the EU and had not adequately provided a response to some complaints by data subjects.

What are the most relevant data protection developments foreseen upcoming in the next months?

The inspections of the Italian Supervisory Authority (Garante)

The Italian Supervisory Authority (Garante) has focused - in the first semester of 2022 - its inspections activities on: (i) processing by data brokers; (ii) processing with the use of cookies; (iii) use of video surveillance; (iv) meeting apps, data monetization, smart toys; (v) artificial intelligence; and (vi) use of personal data by apps. It can be expected that in the next months the Garante will issue some decisions concerning the above-mentioned areas/topics.

In its decision dated 21 July 2022 the Italian data protection authority has published its inspection plan for the second semester of 2022, deciding to focus in particular on: (i) processing of personal data carried out by digital identity managers and by suppliers in the context of apps and online services offered by the Public Administration; (ii) correct application of the guidelines on cookies and other tracking tools; and (iii) transfers of personal data outside of the EU by the use of Google Analytics.

Codes of conduct

Codes of conduct concerning the following aspects will likely be approved in the coming months: (i) telemarketing; and (ii) the processing by general practitioners and pediatricians.

The whistleblowing Italian legislation

Italy has not yet adopted the national law implementing the Directive EU 2019/1937 on the protection of persons who report breaches of Union law. With the law n.127/2022 ("Legge di delegazione europea 2021") the Parliament empowered the government to transpose such Directive by adopting a legislative decree on the matter, amending the regulatory framework of Law No 179/2017. The relevant law in Italy is expected to be approved within the next months and could contain provisions concerning data protection aspects.

National cybersecurity

Italy has already approved a number of laws and regulations concerning cybersecurity. The Law Decree 82/2021 has redesigned the national cybersecurity architecture through the establishment of the National Cybersecurity Agency to protect the national cyberspace. This agency, that has recently started a collaboration with the Garante, has just started to be operational and in the upcoming months will start carrying out its functions.

The Netherlands

Contacts

Maaike van Velzen

Partner

mvanvelzen@deloitte.nl

Marlieke Bakker

Manager

mabakker@deloitte.nl

What are the most relevant **data protection updates of the last months**?

- The Dutch data protection authority (DPA) created a new report form for data breaches which makes it easier to report a data breach to the Dutch DPA. (1 June 2021)
- The Dutch DPA published guidance on the position of the DPO: the different roles, responsibilities and processes (in Dutch). (24 June 2021)
- National case law about the obligation to provide identifying information to IP rights holders. In 2021 (25 June 2021), the Dutch Supreme Court upheld the decision of the Court of Appeal of Arnhem-Leeuwarden that an access cable operator is not required to provide the identifying information of its customers (uploaders) to a film distributor. The right of its customers' protection of their privacy outweigh the rights holder's right to protection of its IP, amongst others because insufficient safeguards were in place. In 2022, in two different cases (2 February 2022 and 9 June 2022), the District Court of Midden-Nederland ruled that the cable operator is not required to send a warning letters from collective organization of rights holders BREIN to its customers because it is not clear if the specific customers infringed the specific IP rights. Even if there would have been an infringement, there is no ground for BREIN's claims as the operator does not have a license (yet) from the Dutch DPA to send warning letters / to provide identifying customers data.
- The Dutch DPA imposed a fine of €450,000 to the Employee Insurance Agency ('EIA') (in Dutch: Uitvoeringsinstituut Werknemersverzekeringen). The EIA had not properly secured the sending of group messages via the so-called 'My Work Folder' environment, where job seekers can communicate with the EIA. There were several data breaches, including concerning health data, of more than 15,000 people. (7 July 2021)
- The Dutch DPA guidelines for cross-sectoral blacklists (in Dutch). The key principle is that cross-sectoral sharing of personal data on a blacklist between private parties is not allowed, unless the GDPR requirements are met. (15 July 2021)
- The Dutch DPA has fined a video hosting service €750.000 for violating the privacy of young children. The information that Dutch users – mostly young children – received from the company when installing and using the app was in English and therefore not easy to understand. By not offering the privacy statement in Dutch, the company did not adequately explain how the app collects, processes and further uses personal data. This is in violation of privacy legislation, more specific the principle that it must always be clear what happens to your personal data. (22 July 2021)

What are the most relevant **data protection updates of the last months**?

- The Dutch DPA published recommendations for the development of so-called smart city applications (in Dutch). These recommendations are intended for municipalities that collect data in public space with smart sensors and measuring equipment. According to the Dutch DPA, the guidance is needed because municipalities do not always pay sufficient attention to privacy legislation, while this is essential for smart city applications that process personal date of citizens. (30 July 2021)

- The Dutch DPA granted more than 160 financial institutions a license to – under strict conditions – register personal data of fraudsters and to share them amongst each other in an incident warning system. The conditions for the data exchange are set out in the Protocol Incident Warning System Financial Institutions. (20 August 2021)

- The Dutch DPA, Dutch Authority for Consumers and Markets, Dutch Authority for the Financial Markets and the Dutch Media Authority, announced that they will cooperate more intensively to strengthen the supervision of digital activities. They started the so-called Digital Supervisors Collaboration Platform. (13 October 2021)

- The Dutch DPA has imposed a fine of €400,000 to an airline operator for failing to protect personal data. Due to poor security, a hacker accessed the operator's systems in 2019 with personal data of 25 million people. The hacker downloaded the personal data of about 83,000 people. (12 December 2021)

- The Dutch DPA imposed a fine of €2.75 million to the Dutch Tax Customs Administration (in Dutch: de Belastingdienst). According to the DPA, the Tax Customs Administration has processed the (dual) nationality of applicants for childcare allowance in an unlawful, discriminatory and therefore improper manner, which constitutes in a serious violation of the GDPR. (7 December 2021)

- The Dutch Supreme Court ruled that the processing of personal data in the context of the credit registration system by the Credit Registration Office (in Dutch: Bureau Krediet Registratie) can be based on legitimate interest, and not legal obligation. This means that the data subject has the right to object under the GDPR, but such an objection does not mean that the data subject's credit registration expires. (3 December 2021)

What are the most relevant **data protection updates of the last months**?

- The Administrative Jurisdiction Division of the Council of State ruled that although the loss of control over personal data constitutes an interference of someone's personality right, this does not mean that that a breach of the GDPR automatically implies that there is an interference of the integrity of a person and thus that there is a legal ground for damages. A data subject must sufficiently demonstrate that there is an interference in person and must proof the claimed damages with concrete information. (26 January 2022)

- The Council of State ruled on the enforcement of data breach reports. A data subject cannot force an administrative body to submit a (GDPR) data breach notification to the administrative court as an administrative decision is required. However, the person concerned can go to the administrative court for a claim for damages. The damage must then be well substantiated. (2 February 2022)

- The Dutch DPA imposed a fine of €525,000 on a media company because data subjects who wanted to access their personal data, or have it removed, were required to upload an identity document. According to the DPA, requesting such information is not necessary in this situation and is too much of a risk. Loss of such information can lead to identity fraud. (24 February 2022)

- The Dutch Supreme Court ruled in a GDPR matter that in the event of a clash between privacy and freedom of information, a balancing of interests must take place. The fact that the applicant is ordered to pay the costs of the proceedings, as this generally concerns only a relatively limited lump sum, is also not in conflict with the right to an effective remedy under the GDPR. (25 February 2022)

- The Spanish privacy regulator Agencia Española de Protección de Datos (AEPD) imposed a €240,000 fine on a recruitment agency, because people who wanted to see their data had to send a full copy of their identity document, among other things. The AEPD started the investigation after a complaint from a Dutch person. The fine was therefore coordinated with the Dutch DPA. The complaint was first filed with the Dutch DPA, but the decisions of the recruitment agency in this area were made in the Spanish branch of the company. Therefore, the Spanish regulator conducted the investigation into the recruitment agency. (21 March 2022).

What are the most relevant data protection updates of the last months?

- The Dutch DPA advises Dutch websites to stop using the advertising system from a European advertising body and advises to use other systems . According to the DPA, the way the advertising body's system collects personal data is in violation with the GDPR. The DPA suggests, as an alternative placing ads based on a website's target audience. The DPA's advice follows on a decision of the Belgian DPA that the system is in violation with the GDPR. (7 February 2022).

- The Administrative Jurisdictional Division of the Council of State assumes that the right of access entitles one to an overview of the processed personal data. The earlier broader interpretation by the Court of Appeal of The Hague does not change this. Moreover, the right of access is not intended to check whether the administrative body followed the correct procedure. This follows from a fraud investigation case. (2 March 2022).

- The Administrative Jurisdictional Division of the Council of State assumes that the right of access entitles one to an overview of the processed personal data. The earlier broader interpretation by the Court of Appeal of The Hague does not change this. Moreover, the right of access is not intended to check whether the administrative body followed the correct procedure. This follows from a fraud investigation case. (2 March 2022).

- Network management in the Netherlands has drawn up 'the smart network management code of conduct' (in Dutch). This code of conduct concerns the processing of personal data (measurement data) for the legal task of network operators. The Dutch DPA approved this code of conduct. (3 May 2022).

- The Dutch DPA published guidelines for members of municipal councils to understand the basics of the GDPR (in Dutch). It is a tool for members of municipal councils to investigate the municipal executive's administration of the municipalities, in particular privacy related decisions. (18 Maoy 2022)

- The Dutch DPA published its annual report on data breaches. In 2021, there were almost twice as much data breaches compared to 2020. (24 May 2022)

- The Custom Administration of the Netherlands must stop using the Citizen Service Number (BSN) in the EORI number of self-employed persons with a sole proprietorship. The Dutch Data Protection Authority has reported that the Custom Administration of the Netherlands has no legal basis to use the citizen service number in the EORI number. (6 July 2022)

- The Dutch DPA advised to amend the proposed Reuse of government information Act (in Dutch: Wet hergebruik van overheidsinformatie). The proposed act does not sufficiently limit the reuse of government information. (11/8/2022)

- The Dutch DPA objects to the proposed Future Accountancy Sector Act (in Dutch: Wet toekomst accountancy sector) that should make the accountancy industry more transparent. According to the Dutch DPA, the proposal infringes the privacy of accountants. (4/10/2022)

- The Dutch DPA objects to the proposed amendments to the Dutch anti money laundering law (in Dutch: Wet plan van aanpak witwassen). According to the Dutch DPA, it would 'open the door to unprecedented mass surveillance'. (21/10/2022)

What are the most relevant data protection developments foreseen upcoming in the next months?

✓ Several European DPA's completed investigations into the use of Google Analytics by websites in several EU member states. The Dutch DPA has completed its investigation on Google Analytics and made a report of the findings. A legal procedure is still pending at the Enforcement Services of the Dutch DPA. After that, the Dutch DPA expects to be able to state whether the use of Google Analytics is permitted or not. The report will be published in 2022. Link to manual for privacy safe Google Analytics (in Dutch).

✓ The Dutch DPA believes that masking personal data in Land Registry and Trade Register is necessary against doxing. According to a new legislative proposal, people can be prosecuted under criminal law for publishing someone's personal data to intimidate them. To combat this so-called doxing, the Dutch DPA finds it also necessary that the government itself stops making residential addresses easily accessible via the Land Registry and the Trade Register without good reason. Link to statement (in Dutch)

✓ The Dutch DPA published a document at the end of 2019 with their focus areas for 2020-2023. These focus areas are:

- Data trade: Data is making products and services more intelligent, which results in these products and services creating more data. Advantages are that such data can be used, for example, offering targeted products and services. It also has disadvantages: there is an increasing amount of unauthorized reselling of personal data to third parties, which can be used to influence and steer people. This is happening both nationally and internationally. (Areas of focus: supervision of data resale, internet of things, profiling and behavioral advertising).
- Digital government: Central and local governments, governmental organizations and the police and the justice department have a large amount of – often sensitive and special – personal data at their disposal. The government is working in a targeted way to use personal data. (Areas of focus: data security, smart cities, partnerships, elections and microtargeting).
- Artificial Intelligence and algorithms: More companies and organizations are using algorithms and AI. This offers benefits and leads to new and useful applications. The use of AI and algorithms also present risks and harmful effects. The Dutch DPA supervises in the field of AI and algorithms when personal data is used. (Area of focus: system of supervision).

Norway

Contacts

Bjorn Ofstad

Partner

bofstad@deloitte.no

Hanne Pernille Gulbrandsen

Partner

hgulbrandsen@deloitte.no

What are the most relevant data protection updates of the last months?

Decisions of the Norwegian data protection authority (Datatilsynet)

2022 - Datatilsynet issued sanctions in several separate cases relating to credit assessments, among others:

September 2022 - A company was issued a fine of 200,000 (€20,000) for carrying out a credit assessment of a person without a lawful basis as the person had no client relationship or other relationship with the company at the time of the assessment.

August 2022 - A fine of NOK 300,000 (approximately €30,000) was issued to a company that carried out credit assessments of two people who did not have any kind of customer relationship or other connection to the company. The reason for the fee is that the company did not have a legal basis for processing the personal data.

June 2022 - Datatilsynet issued a fine of NOK 40,000 ((approximately €4,000) to a company which unlawfully performed a credit rating of a sole proprietorship. Credit information about a sole proprietorship also constitutes personal data, as the owner is immediately identified with the enterprise, and the enterprise is directly linked to the owner's personal finances.

June 2022 - Datatilsynet banned the processing of personal data by the browser extension «Shinigami Eyes», as the processing does not have a legal basis and insufficient information is provided to the data subjects. The "Shinigami Eyes" browser extension seeks to highlight whether content and individuals online are trans-friendly or transphobic.

December 2021 - Datatilsynet imposed an administrative fine of NOK 65 million (approximately €6.5 million) against a social network for not complying with the GDPR rules on consent. The Norwegian Data Protection Authority concluded that the social network disclosed user data to third parties for behavioral advertisement without a valid legal basis. The data shared was GPS location, IP address, Advertising ID, age, gender and the fact that the user in question was on the social network. The social network has lodged an appeal against this decision.

What are the most relevant data protection updates of the last months?

Datatilsynet also issued several sanctions due to data breaches caused by insufficient security measures, among others:

June 2022 - The Norwegian national parliament (Stortinget) was exposed to a data breach in the autumn of 2020, and Datatilsynet subsequently announced a fee of NOK 2 million to the parliament in January 2022. In its response, Stortinget points out that its IT security at the time must be seen in light of the fact that they were strongly affected by the pandemic and the COVID-19 shutdown. Datatilsynet maintained the fee after assessing Stortinget´s response, placing particular emphasis on the fact that Stortinget had not established two-factor authentication or similarly effective security measures to achieve sufficient protection.

June 2022 - Datatilsynet fined the municipality of Østre Toten NOK 4 million (approximately €400,000) after a serious cyberattack resulting from fundamental cybersecurity flaws. The shortcomings related to both log and log analysis, securing backups and lack of two-factor authentication or similar security measures. The firewall was sparsely configured with regard to logging, and a lot of internal traffic was never logged. Servers were not configured to send logs to central log reception and also lacked logging of important events. Furthermore, the municipality lacked protection of backup copies against intentional and unintentional deletion, manipulation and reading. Datatilsynet considered the data attack to be particularly serious because it affected a significant part of the municipality's data, control over personal data was completely lost and information was shared on the dark web to an unknown extent.

Other news from Datatilsynet:

- ✓ Line Coll became the new Director-General of Datatilsynet in August 2022. She announced a new direction with a greater focus on pragmatic guidance for businesses to make it easier to stay compliant.
- ✓ The Norwegian Government's budget proposal for 2023 will make the Norwegian Data Protection Authority's regulatory sandbox permanent. A fourth round of applications for the sandbox was announced in October.

What are the most relevant **data protection developments foreseen upcoming in the next months**?

- The Norwegian government has sent out a consultation proposal on changes to the Police Act, the Police Register Act and the regulations. It is proposed, among other things, to enable the Norwegian Police Security Service to store, systematize and analyze large amounts of openly available information for intelligence purposes. The proposed changes entail that the entire open internet, with online newspaper articles, open public registers, open discussions in social media, comment fields, blogs and more, will be able to be stored and monitored with algorithms and search engines.

- Like many other data protection authorities in the EEA, the Norwegian DPA is currently assessing a complaint made by NOYB regarding the legality of a search engine's analytics. We might see a decision within the next 12 months.

- Also like many other EEA countries, the Norwegian Consumer Council has filed a complaint to Datatilsynet regarding a search engine, claiming that it manipulates users into choosing the least privacy-friendly options through design and misleading information. Datatilsynet will be working together with other Data Protection Authorities on the case.

- The Norwegian Digitalization Agency (NDA) published guidance on data transfers. The guidance has been interpreted as less restrictive in some areas than the guidance from the Norwegian DPA and the EDPB, seemingly allowing for a risk-based approach to transfers. The NDA is a public sector organization which aims to accelerate and coordinate digitalization in the Norwegian public sector.

- The Norwegian Privacy Commission presented its report on the status of privacy in Norway on 26 September. The Commission was established in 2020 to survey the status of privacy and to highlight the most important challenges and trends, in particular in education, the justice system, the public sector and for consumers. The Commission concludes that the digital transformation of Norwegian society has come at the expense of privacy and calls for a national privacy policy. The report contains 140 proposals for measures to improve privacy in Norway, such as pooling privacy resources to make it easier to negotiate with cloud service providers and measures to protect children from the negative effects of digitalization.

Spain

Contacts

Rodrigo Gonzalez Ruiz

Partner

rgonzalezruiz@deloitte.es

Carlos de Jorge

Associate

cdejorge@deloitte.es

What are the most relevant **data protection updates of the last months** (e.g., data protection laws and regulations, guidelines, decisions and sanctions)?

Guidelines issued by the Spanish Data Protection Agency (AEPD):

Guidelines on the personal data processing for HR purposes:

The AEPD has published specific guidelines to be considered by the data controllers in their relationships with their employees. The main topics to be highlighted in this regard are the following:

- ✓ The processing activities for the evaluation of job applicants can be legitimated, in general terms, in accordance with the legal basis established in Article 6.1.b) of the GDPR. The AEPD considers that this processing of activities are necessary in order to take steps at the request of the data subject prior to entering into a contract.
- ✓ The role of the companies who evaluate job applicants on behalf of their clients (HR consultants, headhunters) will depend on the context in which the third party looks for applicants:
- ✓ If the HR consultant or colocation agency maintains a specific agreement with its client in order to look for applicants for specific job offers issued by the client, such HR consultant will be configured as a data controller. The HR consultant receives specific instructions in order to look for candidates for a particular job offer.
- ✓ If the HR consultant looks for candidates in a prospective way (i.e., by using its own databases), without prior instructions provided by the client of the HR consultant's services or without a specific job offer, in general terms, the HR consultant will act as a data controller.
- ✓ Temporary work companies always have to assume the role of data controllers.
- ✓ The use of monitoring technologies in order to control the activity developed by the employees of a company (such as geolocation, video surveillance) has to be previously justified, has to be proportional in order to the purposes to be complied and must be adequately legitimated.
- ✓ In general terms, the employer cannot process personal data concerning the health of its employees. A company can only know the aptitude or inaptitude of an employee to access a job regarding the security and health conditions for such work (work risks prevention).
- ✓ The implementation of whistleblowing channels and the compliance with legal obligations such as a (i) maintain a horary register of the working hours of the staff, (ii) maintain a salary register of the staff (under equality purposes), or (iii) the measures to be adopted regarding victims of gender-bases violence.

What are the most relevant **data protection updates of the last months** (e.g., data protection laws and regulations, guidelines, decisions and sanctions)?

Guidelines issued by the Spanish Data Protection Agency (AEPD):

Guidelines on the notification of data breaches:

The AEPD has published specific guidelines to be considered by the data controllers and the data processors regarding the notification of data breaches to the supervisory authority or the data subjects (Articles 33 and 34 of the GDPR). In general terms:

- ✓ The AEPD provides specific guidelines and criteria in order to calculate the risk involved in a data breach, regarding the personal data involved, its volume, the categories of data subjects, the implications of the data breach and, most important, the possible consequences that may occur regarding the context of the data breach (cyberattack, loss of personal data, lack of availability of the personal data, etc.).
- ✓ Regarding the data subjects, the AEPD has created and published a specific tool to calculate the risk involved in a data breach in order to evaluate the notification of such breach to the data subjects (such tool is named “Comunica-Brecha RGPD”).

Guidelines on managing risk involved in personal data processing (previous risk analysis and PIA):

- ✓ This document is a guide for the management of risks to the rights and freedoms of data subjects applicable to any processing, regardless of its level of risk. In addition, and in the case of high-risk processing, it incorporates the necessary guidelines for carrying out a Data Protection Impact Assessment (DPA) and for the (DPA) and, where appropriate, the prior consultation referred to in Article 36 of the GDPR.

What are the most relevant **data protection updates of the last months** (e.g., data protection laws and regulations, guidelines, decisions and sanctions)?

Relevant sanctions imposed by the AEPD:

PS/00267/2020 (2022/02/11):

- The AEPD imposed to the data controller (marketplace platform) a fine of €2 million for the infringement of Article 10 of the GDPR. The company requested an official certificate of criminal records from the employees of their subcontracted shipping companies, in order to verify that the driver has not been sentenced for the commission of any crime related to road safety.
- The AEPD understood that the data controller was not legitimated to process this type of personal data, regarding that the processing of personal data regarding criminal offences is reserved to certain public authorities and determined situations that were not applicable to such controller. Additionally, the AEPD reminds the claimed company that the employees requested to facilitate the abovementioned certificate were not data controller's employees, regarding that such data subjects maintained their labor relationships with the subcontracted shipping companies.
- The sanctioned data controller was also claimed for a possible infringement with regard to the performance of international transfers. In this point, the AEPD understood that the data controller, acting as a data exporter, complies with GDPR considering that the company had signed the adequate standard contractual clause (SCC). However, the AEPD did not analyze other requirements such as the transfer impact assessment or the adoption of supplementary measures in order to make the SCC enforceable.

PS/00120/2021 (2021/07/26):

- The AEPD imposed to a data controller (supermarket) a fine of €2.5 million for the infringement of Articles 5, 6, 9, 12, 13, 25 and 35.
- The AEPD detected that data controller installed in its supermarkets several cameras with facial recognition in order to identify a potential criminal that has been previously condemned by the competent courts. However, the AEPD pointed that the measure adopted was not proportional and lawful (there was not any applicable legal basis), did not comply with the transparency principle and the risks involved in the processing activities had not been appropriately analyzed.

What are the most relevant **data protection updates of the last months** (e.g., data protection laws and regulations, guidelines, decisions and sanctions)?

Relevant sanctions imposed by the AEPD:

PS/00001/2021 (2022-02-01)

- The AEPD imposed to a data controller (communications service providers (CSP)) a fine of €3.9 million for the infringement of Article 5.1.f) (integrity and confidentiality principle) and Article 5.2 (accountability).
- The AEPD detected that the CPS had not implemented appropriate security measures in order to avoid the 'SIM swapping', which implies that a data subject, by using certain personal data of the CPS' client and supplanting them, were able to request and achieve a duplicated SIM card and, with this, access to the other online services, causing banking frauds, illegitimate purchases, etc.
- The AEPD understood that the CPS did not comply with the data protection regulations regarding the adequate identification of the data subjects when requesting services such a duplicated SIM card.
- In this regard, the AEPD has also published a specific report evaluating the data protection implications and safeguards to be considered to detect, prevent and/or avoid SIM Swapping fraud cases. We are at this moment analyzing the indications provided in such report.

PS/00120/2020 (2022/05/18):

- The AEPD imposed a fine of €10 million on a global technology company for the infringement of Articles 6 and 17 of the GDPR, for the inadequate manage of the right of erasure (right to be forgotten) and for the transfer of personal data to a third party without prior consent of the data subject or without any other legal basis that could legitimized the communication of such information.

What are the most relevant **data protection updates of the last months** (e.g., data protection laws and regulations, guidelines, decisions and sanctions)?

Code of Conduct for the insurance sector:

✓ The AEPD has recently approved the Code of Conduct (CC) for the insurance sector, that has been led by the relevant association of this sector for Spain (in Spanish, "UNESPA"). This CC specifies the data protection legal framework for the insurance companies that are members of the CC, particularizing certain obligations that are more relevant for these entities, such as the processing of health data, data sharing between insurance companies for purposes related to the avoidance of fraud, or specifying how to comply with the data protection principles about each information system used by the insurance companies. This CC also defines determined templates for the compliance with obligation such as the duty of information (providing templates to be includes in the insurance agreements) or the adequate management of data protection rights (providing templates for the exercise of each right and templates to be used a standard response to the mentioned request).

New guidelines or tools issued by the AEPD:

✓ The AEPD has recently designed and published a specific tool to help data controllers to decide whether, considering the risks involved, a data protection breach must be notified to the supervisory authority (La AEPD lanza una herramienta para ayudar a los responsables a decidir si deben notificar una brecha de datos a la autoridad de control | AEPD). This tool complements a specific tool (also designed by the AEPD) to help data controllers to decide when the data protection breach must be notified to the data subjects.

✓ The AEPD has published a specific tool (that has been translated from the tool published by the Supervisory Authority of Singapore) to help data controllers and processors to perform processing activities involving the anonymization of personal data in order to avoid the re-identification of the data subjects. This tool is intended to be used for non-complex situations (i.e.: anonymization for start-ups and small and medium companies).

✓ In this regard, the AEPD has also translated (from the guidelines published by the authority of Singapore) and published specific guidelines concerning the topics, warrants and limitations to perform processing activities involving the anonymization of personal data. These guidelines include specific mention to when must be considered that a specific information does not allow the re-identification of the data subjects and when such information must be considered as pseudonymized data.

Guidelines concerning anonymization activities:

✓ The AEPD has recently published a document containing the main guidelines to be considered in order to perform anonymization activities. These guidelines have been translated from the original document conducted by the Singaporean supervisory authority.

What are the most relevant **data protection developments foreseen upcoming in the next months** (e.g., data protection laws, guidelines, codes of conduct, sectors/areas of inspections)?

Next relevant topics:

- ✓ Spain is evaluating the approval of a specific law in order to guarantee the appropriate protection of whistleblowers that report any potential infringement of the EU regulations and/or any potential criminal offence or administrative infringement caused by a legal person, public administration, its directives or public offices. This law intends to transpose the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

- ✓ The Spanish Data Protection Agency is preparing a particular report on the use of web tracking tools (such as cookies or pixel for analytics purposes) and its implications regarding privacy, especially considering the regulatory framework of international transfers.

- ✓ The AEPD has also recently drafted, with the collaboration of the European Data Protection Supervisor, a specific report to clarify the main common mistakes, in data protection terms, that could be identified in the use of machine learning systems.

Sweden

Contacts

Maria Lilliestierna

Partner

mlilliestierna@deloitte.se

Martina Ljunge

Senior Manager

mljunge@deloitte.se

What are the most relevant **data protection updates**?

Judgments and decisions

Swedish Bank – Administrative fee of SEK 7,500,000

In March 2022, the Swedish Authority for Privacy Protection (in Swedish: Integritetsskyddsmyndigheten) (”IMY”), issued an administrative fee of SEK7,500,000 (approx. €700,000) against a bank due to non-compliance with a several provisions of the GDPR. A central short-coming was the bank, according to IMY, did not provide information on the purpose for which and on which legal basis personal data was processed in one of the company's services. The company also provided incomplete and misleading information about who were the recipients of different categories of personal data when data was shared with Swedish and foreign credit information companies. Furthermore, the bank did not provide information on to which countries outside the EU/EEA personal data were transferred to, or on where and how individuals could obtain information on the safeguards that applied to the transfer to third countries. IMY also noted that the company provided incomplete information about the data subjects' rights, including the right to delete data, the right to data portability and the right to object to how one's personal data is processed. The decision has been appealed by the bank.

Swedish Customs - Administrative fee of SEK 300,000

In March 2022, IMY issued an administrative fee of SEK 300,000 against the Swedish Customs due to deficient routines and insufficient technical barriers, which has led to data from criminal investigations being transferred from staff mobile phones to a US cloud service. A couple of employees at the Swedish Customs' law enforcement activities have used a cloud service on their staff mobile phones, despite not being permitted. The officials had linked their private photo accounts to their mobile phones, which automatically synced the photos and videos taken in their official duty to the cloud service. IMY stated that the Swedish Customs had not taken appropriate technical and organizational measures to prevent what happened, and that there need to be clear routines and guidelines for employees' use of company mobiles and that employees also need to receive training and information on how personal data may be processed in the mobile phones. There should also be technical restrictions for which apps that can be downloaded to the staff mobiles.

What are the most relevant **data protection updates**?

Region of Uppsala - Administrative fee of SEK 1,900,000

In March 2022, IMY issued an administrative fee of SEK 1,900,000 (approx. €175,000) against the Region of Uppsala due to insufficient security measures with regards to its handling of sensitive personal data. The first part of the fine relates to Region Uppsala sending emails containing sensitive personal data and social security numbers to health care administrators, researchers and doctors within the region. As the actual transmission of the email was encrypted but not the information in the emails, IMY concluded sufficient security measures was lacking. The second part of the fine relates to Uppsala University Hospital sending emails with patient data to patients and remitters in third countries (i.e., countries outside the EU/EES) and the storage of patient data in the hospital's email server. More specifically, IMY examined the undertaken security measures but not the legality of the third-country transfer itself. As the information in the emails was not encrypted and was stored in an email-system exposed to the public internet, IMY concluded sufficient security measures were lacking.

Five health care providers – Administrative fees of SEK 22,500,000

In December 2020, IMY issued administrative fees and orders to undertake measures against five Swedish health care providers. According to IMY, the health care providers had processed personal data in breach of the GDPR by making the data available to employees via a record system without carrying out a proper risk analysis. However, IMYs decision was appealed to the Supreme Court (in Swedish: Kammarrätten) which decided to withdraw all issued administrative fees. The Supreme Court also withdrew all orders to undertake measures except for one. According to the Supreme Court, the processing of personal data within the health care system is governed by multiple legislations which concerns both the need for patient data to provide good and safe care, and individuals right to protection of their personal data. Reconciling such legislations is a complex task and IMY had not been able to prove that the health care providers had failed to comply with their obligations under the GDPR.

What are the most relevant data protection developments foreseen upcoming?

Legal statements from IMY

IMYRS 2021:1 – Guidance addressing the meaning of the term "personal data relating to criminal convictions and offences"

In December 2021, IMY published a legal statement addressing the meaning of the term "personal data relating to criminal convictions and offences" under Article 10 of the GDPR. In the statement, IMY reviews the legal sources available in the area such as case law from both international and national courts. According to IMY, the application of Article 10 in the GDPR does not require the existence of a conviction. As a result, information revealing that a person is or has been the subject of a police report, a preliminary investigation or a prosecution, is covered by the article. However, not all information relating to suspected offences falls within the scope. The information must have a certain degree of concreteness, for example that it relates to a specific offence or category of offence. According to IMY, the legal statement shall remain valid until further notice and may be subject to change in the event of new guidance from case law or from the European Data Protection Board (EDPB).

IMYRS 2022:1 – Guidance on the right to erasure of search results for publication in the news media etc.

In March 2022, IMY published a legal statement containing guidance on the right to erasure of search results from search engines. According to IMY, the right to erasure is about weighing the arguments for and against removal. Therefore, a balancing test must be performed upon the request of the erasure. If the public interest to access the information in question outweighs the data subject's interest to have the information removed, the request of erasure shall be declined. The starting point is that data subject's rights to have search results removed outweighs the public interest to access the information. However, one argument for not removing search results is if they may lead to a journalistic publication. Additionally, the fact that someone "plays a role in the public life" may also speak against the removal. Once again, IMY highlights that the legal statement shall remain valid until further notice and may be subject to change in the event of new guidance from case law or from the European Data Protection Board (EDPB).

IMYRS 2022:2 – Guidance on the GDPR-exception for journalistic purposes

In June 2022, IMY published a legal statement clarifying the meaning of article 85 GDPR ("Journalistic purposes") on the balancing test between privacy and the right to freedom of expression and information. According to IMY, the exception to GDPR for "journalistic purposes" does not apply to search services aimed at the public regarding criminal convictions. The exception for journalistic purposes also does not normally cover publication of information of a purely private nature.

What are the most relevant data protection developments foreseen upcoming?

Upcoming developments

IMYs investigation of Swedish pharmacies

In May 2022, Swedish media reported that several pharmacies had sent detailed information about their customers and their online purchases to Facebook. Some of the revealed information was considered as sensitive personal data in accordance with Article 9 of the GDPR. The background to sending the personal data to Facebook was that the pharmacies had been using “Facebook pixels” in their e-commerce to improve their marketing. The leaked data included the web customers’ items in the shopping basket as well as their email addresses and telephone numbers. As a result, IMY has now decided to initiate an investigation of three Swedish online pharmacies.

IMYs investigation of alarm company

In April 2022, Swedish media reported that employees within an alarm company, in connection with incoming alarms, has shared footage and images between themselves in various ways. As a result, IMY has initiated an investigation. According to IMY, they will review what instructions are given to employees with regards to how images may be handled and what technical data security measures the company has adopted in form of access control and logs.

IMYs investigation of online health provider

In May 2022, an online health care provider reported a data breach to IMY. The data breach entails from provider’s usage of a Facebook-pixel on two of its websites which in turn has caused the company to transmit personal data to Facebook. As a result, IMY has initiated an investigation to examine the details of the incident and to examine whether the provider is considered a controller or processor with regards to the transmission.

IMYs investigation of Swedish bank

Despite receiving an administrative fee of SEK 7,500,000 (approx.€690,000) in March 2022, an additional investigation against the Swedish bank was launched in September 2022. According to IMY, the investigation aims to examine whether the bank, through its identification requirements, has made it more difficult for individuals to exercise their rights under the GDPR.

United Kingdom

Contacts

Cavan Fabris

Partner

cfabris@deloitte.co.uk

Peggy Anstett

Managing Associate

panstett@deloitte.co.uk

What are the most relevant data protection updates of the last months?

Brexit

As of 31 December 2020, the EU GDPR no longer applies in the UK. The UK has legislated its own version, known as the UK GDPR, which currently has few material differences to the EU GDPR. The EU Commission has adopted an adequacy decision allowing data to continue flowing freely from the EEA to the UK. However, this decision will be reviewed by the Commission in 2024, and if not extended, the UK's adequacy status will expire in June 2025. Separately, the UK has adopted an adequacy regulation allowing data to continue flowing freely from the UK to the EEA.

International Data Transfer Agreement and International Data Transfer Addendum (collectively the "UK SCCs")

In March 2022, the UK SCCs for international data transfers in scope of the UK GDPR came into force. As of 21 September 2022, organizations can no longer rely on the old EU standard contractual clauses in new contracts and must use the UK SCCs instead. For contracts signed on or before 21 September 2022, organizations have until 21 March 2024 to implement the UK SCCs. The IDTA is designed to be used independently, while the Addendum is designed to be used in conjunction with the new EU standard contractual clauses. For organizations that have both a UK and EU presence, we expect that the Addendum will be heavily used to simplify transfer documentation.

Supreme Court decision on class actions claims

The claim was brought by a consumer activist Richard Lloyd, against one of the Big Tech companies. Lloyd alleged that the company was secretly tracking the personal data of approximately 4.4 million Apple iPhone users for several months in 2011 and 2012, with the intent of using that data for commercial gain and in breach of its obligations as a data controller under the DPA.

The UK Supreme Court, in its landmark decision, refused to allow the claimants to seek damages for the loss of control of their personal data, stating that compensation for a 'non-trivial' breach of the Data Protection Act 1998 (now repealed) can only be awarded where the claimant has suffered some form of material damage - such as financial loss or material distress. The court also ruled that while a 'representative action' could be brought to determine liability, it could not be used determine the quantum of damages for financial loss or material distress because these must be assessed on an individual basis. The ruling in this case has been a relief for controllers across the UK as the ruling has in effect discouraged a potential emergence of 'compensation culture' surrounding low value and/or minor infringements of data protection law. It is not expected that Article 80(2) under the UK GDPR would lead to a substantially different outcome.

What are the most relevant data protection developments foreseen upcoming in the next months?

Proposed data reforms

The Data Protection and Digital Information Bill was introduced into the House of Commons in July 2022, but is on hold as of November 2022. The bill proposes a number of reforms to the UK's data protection laws, with the goal of enabling businesses to more effectively harness the value of data while continuing to uphold high privacy standards. If passed, the Data Protection and Digital Information Bill would result in significantly greater divergence between the EU GDPR and the UK GDPR. Some of the key proposed changes are as follows:

Cookies: As a first stage, the UK proposes removing the consent requirement for analytics cookies and similar technologies. These will be treated as "strictly necessary" cookies. The consent requirement would be removed for a wider range of circumstances where the controller can demonstrate legitimate interest for processing the data. The second stage would be to remove the requirement for prior consent for all types of cookies which the government intends to implement once automated technology is widely available to help users manage online preferences. Long term, the government's intention is to move towards an "opt-out" regime for cookies. This means that cookies would be set without seeking consent, however, websites would need to give clear information on how users can opt out.

Accountability framework: The UK proposes removing the following accountability requirements: (a) designation of a data protection officer under Articles 37 to 39 of the UK GDPR; (b) data protection impact assessments under Article 35 of the UK GDPR; and (c) maintenance of record of processing activities under Article 30 of the UK GDPR. Instead, organizations would be required to maintain a "Privacy Management Programme", including the appointment of a suitable senior individual to be responsible for the program, the implementation of risk assessment tools to help assess, identify and mitigate risks, and more flexible record keeping activities.

Data subject access requests (DSARs): The UK proposes changing the current threshold for refusing or charging a reasonable fee for DSARs from "manifestly unfounded excessive" to "vexatious or excessive". This would bring the requirements in line with the UK's Freedom of Information regime.

Brexit Freedom Bill

The Brexit Freedoms Bill was introduced into the House of Commons in September 2022, pursuant to which it is intended that all EU legislation will be amended, repealed, or replaced in the UK. This will end the special legal status of all retained EU law by 31 December 2023. This may result in re-litigating on established principles such as the CJEU's approach in Schrems II.

Cross jurisdictional offerings

Cross jurisdictional offerings

Deloitte Legal privacy and data protection teams can offer a variety of services, providing highly specialized consultancy in all economical sectors and for all sizes of companies and groups.

Some of the cross jurisdictional offerings are:

- ✓ Drafting or reviewing privacy documents and assisting in the implementation of data governance
- ✓ Drafting privacy notices and cookies banners and policies for sites/ecommerce
- ✓ Drafting and negotiating privacy/security clauses, Data Processing Agreements (DPA), Data Transfer Agreements (DTA), Joint Controllership Agreements (JCA) and other contracts
- ✓ Carrying out Data Protection Impact Assessments (DPIA), Legitimate Interests Assessments (LIA) and other privacy assessments, also in relation to the use of new technologies, including Artificial Intelligence (AI) systems
- ✓ Advising on data transfers related matters, carrying out Transfer Impact Assessments (TIA), drafting Standard Contractual Clause (SCC), Binding Corporate Rules (BCR) and Global Data Transfer Agreements (GDTA), supporting in the identification of adequate supplementary measures
- ✓ Supporting in the management of data breaches and of Subject Access Requests (SAR) and other privacy rights
- ✓ Delivering training and awareness sessions to employees and privacy managers
- ✓ Defining audit plans and carrying out the connected activities
- ✓ Supporting in multi-jurisdictional projects and in extraordinary deals
- ✓ Supporting in any procedure involving the supervisory authorities
- ✓ Assisting in any claim or litigation concerning personal data
- ✓ Providing DPO service or supporting the internal DPO

Deloitte.
Legal

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent, and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's more than 345,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.