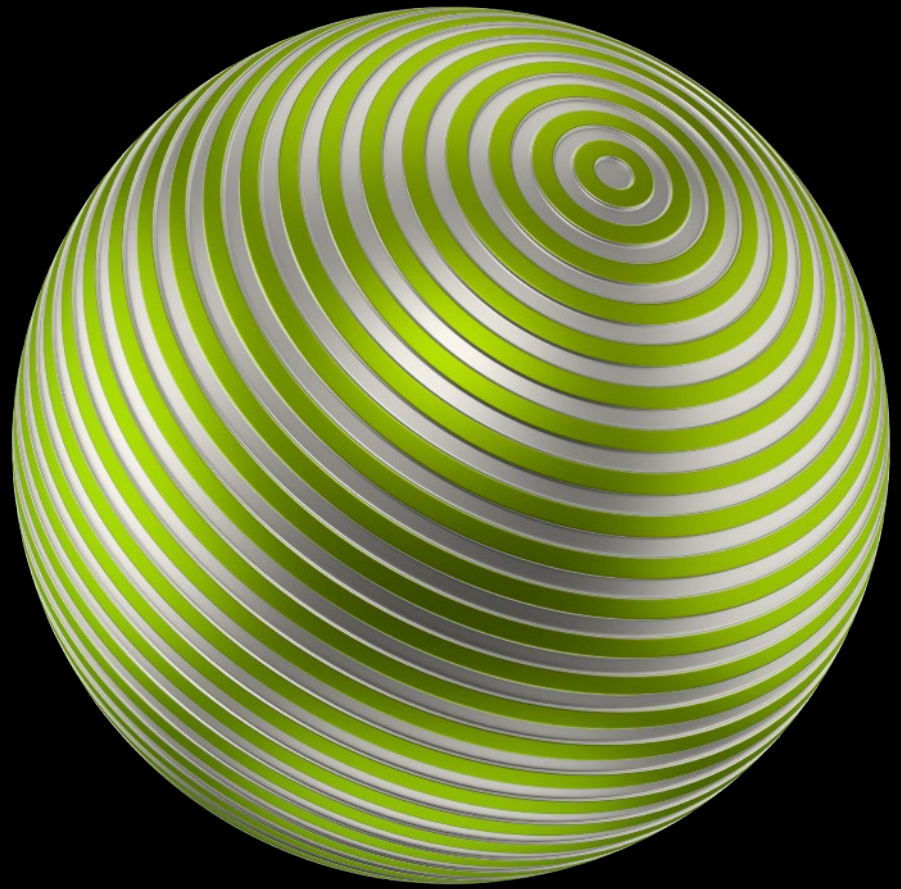
Deloitte.
Legal



Cross-jurisdictional data protection and AI overview

Recent updates and upcoming developments

February 2024 – Second Edition

MAKING AN IMPACT THAT MATTERS since 1845

Index

Introduction

Legal is becoming an essential enabler of the business. That's why you and your executive colleagues need a business advisor pulling in the same direction. Deloitte Legal professionals see the law as empowering, not confining. We help you address the issues that matter most to your organization. We bring business solutions to legal issues and legal solutions to business issues. Plain and simple.

And with us, you get more. Deloitte is at the forefront of emerging technologies, including Generative AI, and continues to build its strong tech-forward reputation. We bring lawyers with experience in technology as well as legal consultants and technologists with access to decades of industry knowledge.

With our global reach and approach, we'll navigate the ever-shifting legal and business terrain together—supporting you every step of the way through unprecedented change and transformation.

Where legal meets business.

Introducing Deloitte Legal and our service

The best of private practice and in-house know how

Global scale with breadth and depth of expertise

We serve leading organizations around the globe across all business domains.

Our legal professionals have a blended skillset, combining legal and business expertise

We provide an ***'enterprise-legal' approach*** delivering a depth and breadth of legal business services, with a focus on People, M&A, Contracting, Intangibles, Dispute Management, Corporate and ESG.

Delivered with a business-first approach

We focus on achieving better business outcomes leveraging our technological and cross-functional expertise.

A different legal perspective

We offer an integrated legal service focused on the delivery of a solution to a business challenge or opportunity leveraging our skills in each of these key areas.

Our services range from legal advisory, to law firm department consulting, through to a full range of managed services. We are inherently global, cross-functional, industry informed, and technology enabled, with a focus on delivering solutions.

One relationship provides endless connections.

A part of Deloitte – we are a Deloitte shaped business with a track record of getting things done

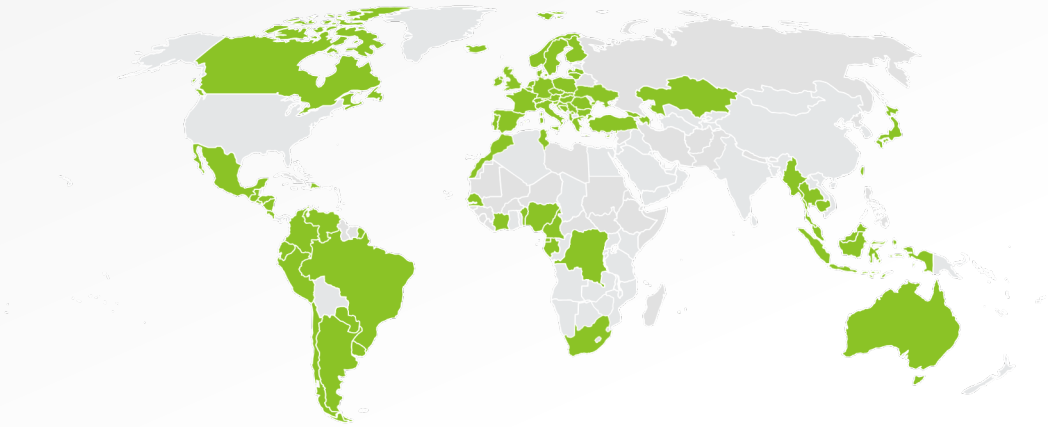
The scale and reach of Deloitte

Housing a global legal business with the same DNA

Deloitte Legal presence

76 countries

2,500+ legal professionals



collaborating seamlessly
across borders and with other Deloitte business lines

Deloitte Legal practices

1. Albania
2. Argentina
3. Australia
4. Austria
5. Azerbaijan
6. Belgium
7. Benin
8. Bosnia
9. Brazil
10. Bulgaria
11. Cameroon
12. Canada
13. Chile
15. Colombia
16. Costa Rica
17. Croatia
18. Cyprus
19. Czech Rep.
20. Dem Rep of Congo
21. Denmark
22. Dominican Republic
23. Ecuador
24. El Salvador
25. Equatorial Guinea
26. Finland
27. France
28. Gabon
29. Georgia
30. Germany
31. Greece
32. Guatemala
33. Honduras
34. Hong Kong SAR, China
35. Hungary
36. Iceland
37. Indonesia
38. Ireland
39. Italy
40. Ivory Coast
41. Japan
42. Kazakhstan
43. Kosovo
44. Latvia
45. Lithuania
46. Malaysia
47. Malta
48. Mexico
49. Morocco
50. Myanmar
51. Netherlands
52. Nicaragua
53. Nigeria
54. Norway
55. Paraguay
56. Peru
57. Poland
58. Portugal
59. Romania
60. Senegal
61. Serbia
62. Singapore
63. Slovakia
64. Slovenia
65. South Africa
66. Spain
67. Sweden
68. Switzerland
69. Taiwan
70. Thailand
71. Tunisia
72. Turkey
73. Ukraine
74. Uruguay
75. United Kingdom
76. Venezuela

Overview

A complex framework, a cross-jurisdictional approach

In today's digital economy, strategic data governance is crucial for businesses of all sizes and operating in any industry. General Data Protection Regulation (GDPR), which came into force in 2018, provided economic operators a uniform legal framework that helped in structuring procedures, documents, contractual relationships, etc. on common basis. Despite this, the GDPR still leaves a wide margin of discretion to EU member states.

Furthermore, the GDPR is now being strengthened by new European Acts that fall under the EU strategic plan for digital transformation, setting standards to shape the digital future of the EU (such as the AI Act, the Digital Markets Act, the Digital Services Act, the Data Act, the Data Governance Act, and the NIS 2 Directive, etc.).

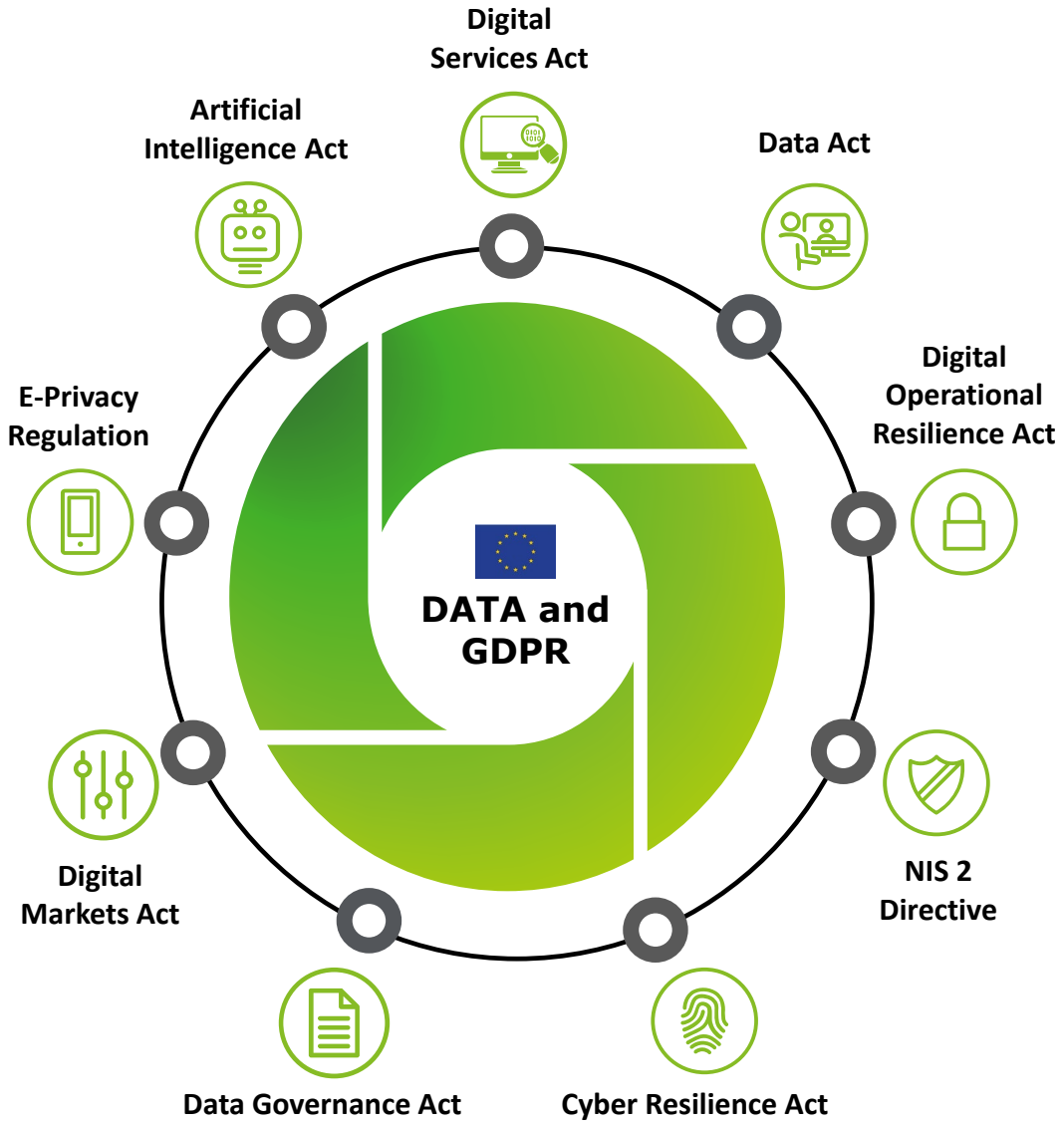
The common denominator in the emerging European legal framework is data, the protection of which remains a cornerstone in the European Union.

Now, after five 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 effective data management within an organization, an integrated approach is therefore fundamental and Deloitte Legal is the ideal partner for that.

This document consolidates an overview across 16 jurisdictions on:

- The most relevant data protection laws, regulations, guidelines, decisions and sanctions of the last months;
- The most relevant AI updates; and
- Some upcoming developments in the data protection and AI fields 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

Albania

Contacts

Ened Topi

Senior Manager, Deloitte Legal Albania

etopi@deloittece.com

Luizita Voda

Senior Associate, Deloitte Legal Albania

lvoda@deloittece.com

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

Short introduction to Albanian data protection legislation (non – EU)

Albania is in the process of making substantial revisions to its data protection legal framework. A new law on personal data protection, anticipated to be approved within next year, will fully incorporate the principles of the GDPR (General Data Protection Regulation).

The Law No. 9887 dated 10 March 2008 "On personal data protection" as amended ("**Data Protection Law**"), currently in force, alongside the framework of decisions, instructions, and guidelines issued by the Information and Data Protection Commissioner ("**IDPC**"), already impose a comprehensive set of regulations for data controllers to adhere to and is generally in line with the principles enshrined in the GDPR.

These obligations encompass requirements for transparency and accountability, including notifying the IDPC about processing activities, informing data subjects before processing commences, and implementing appropriate technical and organizational measures as stipulated by the Data Protection Law and IDPC decisions.

Moreover, the Data Protection Law establishes specific conditions for data controllers engaging in cross-border data transfers, and the IDPC has approved a lists of countries deemed to provide an adequate level of personal data protection. Exceptions permitting cross-border data transfers to countries lacking sufficient protection can only occur under specified conditions outlined in the Data Protection Law.

Decision No. 53 dated 22 November 2023 of the IDPC

The IDPC recently conducted an administrative investigation into a company specializing in the online trading and sale of tickets for various events. The investigation revealed several violations, including the **failure to determine the storage limit** for users' personal data, **lack of transparency** on data processing purposes and methods, lack of clarity in service contracts with data controllers and **lack of data processing agreements**, **incomplete data processing notifications to the IDPC**, and **inadequate organizational and technical measures** to protect personal data. As a result, the IDPC imposed a sanction of approximately €8,600, along with relevant recommendations, emphasizing the importance of compliance with data protection legislation.

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

Decision No. 22 dated 29 May 2023 of the IDPC

The IDPC conducted an administrative investigation into a postal service company, uncovering multiple violations. The controller **failed to determine storage limits**, **lacked a comprehensive and transparent privacy notice** for website users, as well as had submitted **incomplete/inaccurate data processing declarations to the IDPC**.

Furthermore, the controller **lacked adequate organizational and technical measures for data security**. The IDPC imposed a sanction of approximately €6,000 and issued relevant recommendations, highlighting the need for compliance with data protection laws.

Decision No. 03 dated 15 February 2023 of the IDPC

The IDPC conducted an administrative investigation into an insurance company, revealing several breaches of data protection laws.

The IDPC found, *inter* alia, that the controller failed to establish the **storage limits** for users' personal data, **violated CCTV usage transparency requirements**, and lacked transparent **privacy notices** for both website users and data subjects.

Insufficient organizational and technical measures to safeguard personal data were identified, along with a lack of **proper data privacy training for employees**.

As a result, the IDPC imposed a sanction of approximately €3,600, accompanied by relevant recommendations.

What are the most relevant **AI updates**?

Intersectoral Strategy "Digital Agenda of Albania" and the Action Plan for 2022-2026

Based on the Intersectoral Strategy "Digital Agenda of Albania" and the Action Plan for 2022-2026 approved by Decision of Council of Ministers No. 370 dated 01 June 2022, there is a strategic push toward enhanced digitization of public services.

The objective is to enable online responses featuring electronic signatures or seals for all public services offered via the e-Albania government portal, primarily those categorized as applications.

Moreover, the plan includes the integration of cutting-edge technologies such as blockchain and AI, aiming to elevate the overall quality of public services provision.

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

New expected law on data protection fully transposing GDPR

Albania is experiencing substantial transformation in its data protection legal landscape, signaling a proactive response to the evolving global standards.

Anticipated within the next year, a new law on personal data protection will be enacted, fully transposing the General Data Protection Regulation (GDPR).

The new law will introduce more rigid compliance requirements for data controllers, will further elaborate provisions on transparency, accountability and data subject rights, as well as introduce higher sanctions in case of violations of the data protection legislation.

Australia

Contacts

Donna Bartlett

Partner, Deloitte Legal Australia

dbartlett@deloitte.com.au

Gemma Lockyer

Director, Deloitte Legal Australia

glockyer@deloitte.com.au

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

Extraterritorial expansion and penalties under the Privacy Act

In December 2022, the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth) was passed to expand the extraterritorial reach of Australia's Privacy Act 1988 (Cth).

- The amendment amended the 'Australian link' test under the Privacy Act, which determines whether the Act applies to an overseas organization. The test no longer requires overseas entities to hold or collect personal information in Australia. This means the Privacy Act will apply to any organization that carries on business in Australia, regardless of whether they hold or collect personal information in Australia.
- This extended scope includes the application of the civil penalties regime and the powers of the Office of the Australian Information Commissioner (OAIC) to such overseas entities.
- The maximum civil penalty has been significantly increased for serious or repeated privacy offences under the Act. It is now the greater of A$50 million, three times the value of the benefit the body corporate obtained, or 30% of the body corporate adjusted turnover during the breach turnover period.
- The OAIC has been granted greater enforcement and investigatory powers.

This amendment is the first of many prospective reforms to the Privacy Act, as the Australian government is currently reviewing and consulting on additional legislative changes.

Biometric data scraping breached Australia's Privacy Act

In a recent landmark ruling, the Administrative Appeals Tribunal (AAT) handed down its decision that an American facial recognition company's conduct breached the Privacy Act by scraping facial images of Australians from the web and storing the data for biometric identification purposes.

- This case is significant as it confirms the extraterritorial applicability of the recently amended Privacy Act to overseas entities who carry on business in Australia, despite not having a physical presence in the country.
- The AAT determined that Australian Privacy Principals (APPs) 1.2 and 3.3 had been breached. The collected data became sensitive information once acquired and used for biometric identification purposes, and consent had not been obtained. The company had failed to take reasonable steps to implement practices and procedures to comply with the APPs.

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

Data breach class actions

- Multiple class actions have commenced against two Australian organizations, a telecommunications company and a large private health insurance provider, on behalf of customers in response to large-scale data breaches that occurred in late 2022.
- The cyberattacks collectively impacted tens of millions of Australians. The types of data stolen in the breach included medical records, identity documents, and other personal information.
- The claims brought by these class actions allege the organizations' failure to take reasonable steps to protect personal information.
- These class actions are significant because in Australia's history only one data breach class action has ever commenced (and was ultimately settled). These proceedings will establish court precedence and clarify the Australian courts' interpretation of data protection laws.
- As of December 2023, two claims against the health insurance provider have been merged and all proceedings are currently at early stages, meaning a decision or resolution soon is unlikely.
- It also suggests a greater public lens on data protection in Australia, which may inevitably lead to similar proceedings in the future and increase the demand for greater cybersecurity.

What are the most relevant AI updates?

Consultation on ‘Safe and Responsible AI’ rules

Australia has concluded domestic consultation on ‘Safe and Responsible AI’ and received 510 submissions from the public. The Australian government sought to determine how public trust and confidence in AI could be increased, including whether regulatory safeguards are desirable. The government has yet to respond to the submissions received from the enquiry. The Safe and Responsible AI consultation asked a number of questions of respondents including the following:

- What gaps exist in the current state of AI regulation in Australia?
- What are respondents' opinions on foreign jurisdictions’ treatment of AI, including the EU, US, UK, Canada and China?
- Should private company usage and government usage of AI be regulated differently?
- Do respondents support a risk-based approach for regulating AI?

An article written by the Australian Deloitte Legal team breaks down some of the responses and insights from industry. Respondents agreed that there is a gap in current approaches to regulating AI, but were split between needing sector specific AI legislation, similar to the UK proposed approach, or horizontal industry-wide AI regulation like the EU approach. Respondents almost unanimously supported a risk-based approach and agreed that the government required AI standards as much as private enterprise.

Five billion AUD investment in Australia for AI and tech upskilling

The Australian government announced at the Australian embassy in Washington that Microsoft is to invest A$5 billion expanding AI and cloud computing abilities in Australia over the next two years. This represents the largest investment made by a global technology provider in Australia and will:

- Increase the domestic footprint of Microsoft data centers;
- Fund a new education facility which will train 300,000 Australians in digital skills; and
- Allow Microsoft to collaborate with the Australian Signals Department to protect Australians online.

Bletchley Declaration signed by Australia

Australia has signed the Bletchley Declaration, along with a number of other countries and organizations at the UK AI Safety Summit on 1-2 November 2023, to affirm its commitment to work with the international community to encourage the safe, ethical and responsible development of artificial intelligence. This declaration recognizes the importance of collaborating on testing the next generation of AI models against a range of critical national security, safety, and societal risks.

What are the most relevant upcoming data protection developments?

Australian government's response to the review of the Privacy Act

A large-scale review into the Australian privacy regime has entered its final stage with the government response to the Privacy Act Review Report. The Australian government has indicated support in-principle for the majority of recommendations, likely paving the path for further regulatory changes in this space.

The proposed changes intend to clarify privacy obligations for relevant entities and enhance protections for individuals. The key recommendations that will likely have global impact include:

- **The designation of countries with substantially similar privacy laws.** This will facilitate the free flow of data with adequate protections and allow businesses to disclose personal information to recipients in those countries, without the need for contractual measures.
- **The development of standard contractual clauses** for businesses to use when transferring personal information to non-prescribed countries. These clauses would be voluntary and interoperable with those developed in other jurisdictions where possible.
- **Mandate the disclosure of overseas data flows** where entities transfer personal information offshore.
- **The expansion of the Information Commissioner's powers** regarding the civil penalty provisions, and the power to undertake public inquiries/reviews that are approved or directed by the Attorney-General.

Overall, there is a clear direction and focus on improving the data protection framework in Australia.

Additional funding for regulatory bodies

- In the 2023-24 Federal Budget, the Australian government allocated additional funding which has been set aside for the Office of the Australian Information Commissioner (OAIC), the Australian regulator in charge of the Privacy Act 1988 (Cth).
- This additional funding will be used to support privacy activities, including work responding to the increased complexity, scale and impact of notifiable data breaches, as reflected in recent large-scale breaches. This suggests an increasing emphasis on data protection and cybersecurity enforcement in Australia.

Australian Cyber Security Strategy 2023-2030

The Australian Cyber Security Strategy 2023-2030 has recently been released by the Australian government. It proposes several regulatory changes with the aim of establishing Australia as a world leader in cybersecurity by 2030, including:

- Mandatory reporting of ransomware attacks against Australian organizations;
- Enhanced security requirements for critical infrastructure providers in Australia, specifically telecommunications providers;
- Adoption of mandatory cybersecurity standards for digital technologies such as consumer IoT (internet of Things) devices sold in Australia, consistent with international security standards; and
- Building regional capabilities and actively contributing to international legal frameworks through global cooperation to prevent, deter and respond to cybercrime.

Belgium

Contacts

Matthias Vierstraete

Director, Deloitte Legal Belgium

mvierstraete@deloitte.com

Julie Van Com

Managing Associate, Deloitte Legal Belgium

jvancom@deloitte.com

What are the most relevant data protection updates?

Every year, the Belgian Data Protection Authority ("BDPA") shares its list of priorities (Version 2023 available in Dutch and French).
In 2023, the BDPA focused on the following points:

Cookies

Since a fully harmonized position on the European level on all aspects of cookies was lacking at the beginning 2023, the BDPA strived to make its national position on cookies more explicit. The reason for setting this priority was due to the number of complaints about cookies received by the BDPA in 2022 and the launch of the first "thematic investigation" regarding cookies on press websites also in 2022. These elements have led to several decisions about cookies in 2023 (see Dutch and French). In the same context, the BDPA has published a checklist for the correct use of cookies (*infra*).

DPO

The BDPA claims that the DPO is its most important ally in the field of data protection. Therefore, the BDPA continued to support this crucial role. Action took place in terms of preventive actions, in particular, to inform complainants about the role of the DPO in the exercise of their rights when filing a complaint. Furthermore, in terms of monitoring, the Inspectorate examined the place of the DPO in organizations that are the subject of an investigation of the BDPA.

Smart cities

In smart cities, digital technology is used to collect data and through this, the lives of its citizens ought to be improved. Since a vast amount of (personal) data will be processed in this context, this comes with some potential risks. Therefore, the BDPA wanted to provide preventive actions and create dialogue with local actors in the area of smart cities, for instance on the field of intelligent transportation ("**ITS"**).

As a part of the EU Digital Strategy, the European Commission aims to use its ITS solutions in order to achieve a more efficient management of its transport network for passengers and business. Intelligent transportation is an advanced application aiming to provide innovative services relating to different modes of transport, including wireless, electronic and automated technologies. As there are some challenges regarding data protection, the concept has not gone unnoticed by the Belgian BDPA.

Youngsters and data brokers

In 2023 the BDPA continued its awareness-raising project "ik beslis". The "Ik beslis" campaign is aimed at young people on the one hand and at parents and teachers on the other hand. With this awareness project, the BDPA wants to explain the privacy legislation in an understandable language. In this context, the BDPA zooms in on the concept of "data brokers". This is necessary, specifically for young people, since they are often targeted by data brokers. Consequently, the BDPA provides tips and tricks to youngsters and their parents and teachers to surf more safely on the internet.

What are the most relevant data protection updates?

Data protection laws and regulations, guidelines:

In 2023 a Decree was adopted in Flanders, including a legal basis for data sharing between social workers, police and justice in criminal investigations. This new legal basis should allow for an optimalization in the communication of personal data in criminal investigations.

In general

At the Flemish level, a decree has been adopted which forms a new legal basis for the sharing of data in the context of article 458 of the Belgian criminal code (hereinafter the "CC").

Article 458ter CC allows for the existence of a structured consultation between social workers, police and justice. For example, when dealing with intra-family violence and child abuse or to prevent terrorist crimes. More specifically, the article provides for the possibility of such social workings, to break their professional secrecy and to exchange information with police and justice. When it comes to the exchange of personal data however, this was rather complicated, since there was no clear legal basis.

Therefore, the new Decree of 30 June 2023 provides a solution. The decree provides a solid legal basis which allows multidisciplinary cooperation, as well as sharing of personal data when specific organizations, subject to the competence of the Flemish community or region, are participating in a case consultation regarding (i) protection of people and (ii) the prevention of crimes by criminal organizations (cfr. Article 458ter CC).

This is only applicable to organizations which are subject to the competence of the Flemish community or region. Therefore, federal services (such as police and public prosecutors) do not fall under this decree. Only organizations that fall under the competences of the Flemish community or the Flemish region, for instance the houses of justice, can rely on the new legal basis of the decree.

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

Data protection laws and regulations, guidelines:

In October 2023 the BDPA published a checklist about the correct use of cookies.

In general

The BDPA has released a helpful (non-exhaustive) checklist for organizations to ensure their cookie practices align with existing regulations.

As mentioned before, the use of cookies was one of the priorities of the BDPA in 2023. In line with this priority, the BDPA unveiled a comprehensive tool that systematically addresses certain 'dos and don'ts' pertaining to cookies and similar tracking mechanisms.

The guidance underscores *inter alia* that only “strictly necessary” cookies are exempt from requiring consent. For all other cookie categories, placement and retrieval is permitted only if users have provided their prior, freely given, specific, informed, unambiguous, and active consent.

The cookie checklist has become part of the BDPA's toolkit for data controllers, complementing existing resources such as templates for processing activity registers, the DPO checklist, and the overview of data subjects' rights based on legal foundations.

What are the most relevant data protection updates?

Recent cases

12 January 2023: Right to lodge an appeal. The Constitutional Court of Belgium decided that third parties who were not a party to the administrative decision of the BDPA's Disputes Chamber, should be able lodge an appeal at the Belgian Market Court.

24 May 2023: Transfer of tax related personal data. The Dispute Chamber of the BDPA prohibited the Federal Public Service ("FPS") Finance from transferring tax data of people having both the Belgian and US nationality, to the U.S. tax authorities as provided in the Foreign Account Tax Compliance Act ("FATCA-agreement"). Therefore, the BDPA prohibits the FPS Finance from processing the complainants' data. Further, the BDPA request the competent legislator to comply with this prohibition and remedy the shortcomings found.

The FATCA-agreement provides for the exchange of data between X and Y to prevent tax fraud. National financial institutions are required to transfer data on Americans residing abroad to the national tax authority of the country of residence. This exchange of data was found to be in breach of the obligations of the GDPR, since they did not comply with the requirements on transfers of personal data outside the European Union.

The Dispute Chamber also ruled that article 96 of the GDPR should be interpreted restrictively. This article allegedly established a "standstill", meaning that international agreements pre-dating the enforcement of the GDPR may continue to be valid subject to the condition they were in compliance with the relevant legislation at the time of their conclusion.

The "standstill" effect of that article is now limited in this decision, in the sense that, according to the Dispute Chamber, it cannot be intended to allow international agreements to remain in conflict over time with applicable law. The exception for international agreements concluded prior to the implementation of the AVG consequently does not relieve the EU member states from the obligation to (re-)negotiate an agreement in order to bring such agreement in line with the GDPR.

The Disputes Chamber thus concluded that the transfer of personal data of Americans living in Belgium to an agency in a country outside the EU (which cannot provide an adequate level of data protection) is unlawful. It therefore prohibited for the FPS Finance to exchange the personal data of Americans, living in Belgium.

17 May 2023: Recording of customer phone conversations. The BDPA imposed a €40,000 fine on a company for recording its customer phone conversations without their consent and for denying them access to the recordings. The dispute arose from two agreements related to a website development between the parties, leading to a complaint in April 2022.

The BDPA found the company violated the GDPR principles, including the transparency obligation and the right to access of data. As a consequence, the BPDA ruled that article 12, paragraph 1 of the GDPR, emphasizing "appropriate measures" for transparent information, was violated. Besides, their privacy statement required some attention as it failed to clearly specify the categories of personal data, retention periods, and recipients which caused the Dispute Chamber to also conclude breaches of GDPR articles 5, 12, and 13. The decision stressed the data subject's right to understand data processing, and the company's refusal to provide copies, suggesting on-site listening only, violated the GDPR. The provision of transcripts of the recorded conversations alone were deemed insufficient as they couldn't reveal the complainant's voice, which is a fundamental personal data aspect.

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

Recent cases

5 December 2023: Cookie banner and settlement proposal. Recently, the Flemish Radio and Television Broadcasting Organization ("**VRT**") faced a **complaint regarding its cookie banner**. The complainant, being represented by Max Scherms' organization None Of Your Business ("**NOYB")**, claimed that the VRT was using misleading cookie banners and "dark patterns".

NOYB complained that there was no "reject option" at the initial information level of the cookie banner on its website. VRT on the other hand, argued that NOYB had not considered their latest and updated version of the cookie banner, which did include a "reject option". In their new version, a refusal could be made by clicking the "reject all" button. VRT therefore claimed that the complaint of NOYB did not reflect the current situation. Still, in their new cookie policy the "accept all" button was in blue and the "reject all" button in white, which the BDPA did not consider as "equivalent" to each other.

The BDPA then presented a **settlement proposal** ("*schikkingsvoorstel*"), based on article 95, § 1, 2° of the law of 3 December 2017 establishing the (Belgian) Data Protection Authority, to address the concerns raised by the complainant. The settlement proposal included the following elements:

- **A modification of implementation modalities**: the BDPA requested various adjustments to the implementation modalities of VRT's cookie banner, specifically VRT needed to implement a "reject all" button which is equivalent to the "accept all" button.
- **Technical adjustments documentation**: VRT was required to provide a detailed document outlining the technical adjustments that were made during the implementation of the banner.
- **Statement in the settlement proposal:** VRT, requested a statement in the settlement proposal asserting that their agreement with such settlement proposal would not imply admission which could specifically be used as aggravating circumstances in determining the sanction for future proceedings before the Dispute Chamber.

A settlement proposal, based on article 95 §1, 2°, is considered a "*prima facie*-decision" within the procedure preceding the substantive decision by the Dispute Chamber of the BDPA. Therefore, at this stage, the BDPA cannot impose administrative fines (despite the request of NOYB). These kind of settlements aim to provide a comprehensive solution to the grievances raised in the complaint, avoiding punitive measures and fostering compliance with data protection regulations.

The settlement proposal was accepted by the VRT on 1 December 2023 and as from that moment there is now a 30-day period for potential appeals to the Belgian Market Court.

The complaint of NYOB, against the VRT was filed in the context of a large-scale action by NOYB, in which the organization brought **15 Belgian news sites** before the BDPA because of their alleged GDPR violations relating to the use of cookies. Such claims were initiated against, amongst others, some of Belgium's large TV channels like VRT and "RTL Belgium", but also against newspapers like "Het Laatste Nieuws", "La Libre", "L'avenir", and "De Morgen". At the moment (15 December 2023), already five decisions of the BDPA, including settlement proposals, have been published on the website of the BDPA.

Bulgaria

Contacts

Miglena Micheva

Senior Manager, Deloitte Legal Bulgaria

mmicheva@deloittece.com

Irena Koleva

Senior Associate, Deloitte Legal Bulgaria

ikoleva@deloittece.com

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

Whistleblower Protection Act

On 4 May 2023, the new Bulgarian Act on the Protection of Persons Who Report or Publicly Disclose Information on Breaches ("Whistleblower Protection Act", "the Act") came into force. It is the Bulgarian implementation of the EU Whistleblowing Directive (Directive (EU) 2019/1937). The aim of the Act is to create legal certainty and for whistleblowers who help to uncover and punish wrongdoing through their reports. Whistleblowers enjoy the protection of the law, among other things, when reporting violations of personal data protection legislation as well as Bulgarian employment law.

Pursuant to the Act, the obliged entity appoints one or more employees responsible for handling reports - this may be the data protection officer, and if there is no obligation to appoint a data protection officer, another employee is designated to handle reports.

The Commission for Personal Data Protection ("CPDP") is entrusted with the supervisory functions under the Act. It is also a competent body for receiving and organizing externally submitted reports.

Companies and organizations with more than 249 employees must set up and operate a whistleblower system since the effective date. As from 17 December 2023, this obligation also applies to companies with at least 50 employees.

In the process of receiving and processing reports of violations, the obligated entities must take measures to protect confidentiality and personal data.

The Act specifically provides that obliged entities should not process personal data that are clearly not relevant for considering the specific signal. If personal data unrelated to the signal are accidentally collected, they are subject to deletion. In the course of this process, the provisions of the GDPR and the Bulgarian personal data protection legislation apply.

Ordinance on the maintenance of the register of whistleblowers pursuant to the Whistleblower Protection Act

On 4 August 2023, the Ordinance on the maintenance of the register of whistleblowers pursuant to the Whistleblower Protection Act ("the Ordinance") entered into force. It was adopted by the Commission for Personal Data Protection and its aim is to bring clarity to the requirements for the internal register of whistleblowers, which legal entities covered by the Act must maintain.

The Ordinance contains provisions on setting up and content of the register; receipt and processing of reports received through internal channels; maintenance of the register and other requirements. The Ordinance provides that, in certain cases, a report received through an internal channel must be forwarded to the Commission for Personal Data Protection in its role as an external whistleblowing channel.

In addition, the Ordinance introduces a data retention period for storing the report and the respective materials, which is five years after the completion of consideration of the report, except in the presence of criminal, civil, labor law and/or administrative proceedings in connection with the submitted report.

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

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

Opinion of the CPDP on the legality of video surveillance for the purposes of evaluating the performance of employees

On 24 November 2023, the Commission for Personal Data Protection (CPDP) issued an Opinion № ПНМД-17-239/2023 regarding the lawfulness of video surveillance for the purposes of evaluating the performance of the work duties of employees in connection with the determination of their additional labor remuneration.

The CPDP considered a letter from a Bulgarian oil and gas company (the Company), requesting an opinion on the legality of the use of video surveillance and audio recordings for the abovementioned purposes, and was also interested to learn what preliminary actions should be carried out to comply with the GDPR.

The CPDP's analyzed various related aspects, including among others:

- The Company owns a chain of gas stations (objects/gas stations) on the territory of the country, which are subject to video surveillance in order to protect its legitimate interests (security purposes). However, the evaluation of the performance of the employees' work duties for the purposes of determining their additional remuneration is another, subsequent purpose, which is absolutely incompatible with the initial (security) one.
- The planned processing of personal data also refers to activities that fall within the scope of the concept of "profiling", which is regulated by specific provisions of the GDPR and none of the hypothesis apply in this case.

The CPDP's opinion is that the subsequent processing of the recordings from the video surveillance, including audio recording, for the purposes of assessing the performance of the work duties of the employees of the Company, for the needs of determining their additional remuneration, does not comply with the requirements of article 6, paragraph 4 of the GDPR and is therefore inadmissible.

What are the most relevant data protection updates?

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

Sanctions

No major sanctions have been imposed by the CPDP in 2023.

The biggest sanctions imposed by the CPDP so far are the following:

- The National Revenue Agency ('the NRA') was fined BGN 5.1 million (approx. €2.6 million) for leakage of personal data of over six million people due to a hacking attack. The CPDP found that the NRA had not undertaken sufficient technical and organizational measures for data protection.
- A bank was fined BGN 1 million (approx. €512,330) for leakage of personal data of over 33,000 customers in over 23,000 credit files. Due to insufficient technical and organizational measures, third parties had access to personal data including copies of ID cards, tax, and financial documents, health data, etc.
- The NRA was fined BGN 55,000 (approx. €28,180) for insufficient legal basis for personal data processing. Data was unlawfully collected and used by the NRA in relation to an enforcement case against the data subject.
- A telecommunication service provider was fined BGN 53,000 (approx. €27,150) for insufficient legal basis for personal data processing. The provider had repeatedly made registration of prepaid services without the knowledge and consent of the data subject, as the latter had not signed the application.
- Bulgarian Posts PLC was fined BGN 1 million (approx. €510,000) because the company did not implement appropriate technical and organizational measures before and during the cyberattack of 16 April 2022 and thus allowed malware to encrypt sensitive databases.

What are the most relevant data protection updates?

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

Requests for preliminary rulings

An interesting preliminary inquiry (case C-200/23) was referred to the Court of Justice of the European Union (CJEU) in the area of personal data protection by the Bulgarian Supreme Administrative Court (SAC) and concerns the matter of the entry in the Commercial Register and publishing of personal data.

The SAC formulates eight questions, some of which are:

- When the Registry Agency owes compensation for non-property damages for undeleted personal data in the Commercial Register - is it sufficient the very fact of the publication of the data, or noticeable adverse effects should be present which should affect personal interests?
- Pursuant to the provisions of Bulgarian law on Commercial Register and the Register of Non-profit Legal Entities, when the application or documents to it contain personal data which is not required by law, those who have provided those data shall be deemed to have consented to their processing. Are these provisions compliant with the EU legislation?
- Are the signatures under the company agreements personal data?

The case in connection with which the inquiry was made is related to publishing the partnership agreement of a limited liability company, without deleting the personal data of one of the partners. The partner whose data has been published made a request to the Registry Agency to delete his data, but the Agency did not take any action. Case C-200/23 is still in progress.

Court practice

In 2023 the Sofia Regional Court (SRC) confirmed the fine of BGN 5.1 million (approx. €2.6 million) which the Commission for Personal Data Protection (CPDP) imposed on the National Revenue Agency (NRA) after the large leak of personal data in 2019.

In February 2023, the Administrative Court – Sofia-city firmly accepted that the NRA could have prevented data leaks of over six million citizens and legal entities but has failed to act.

The decision of the SRC makes it clear that one of the main data breaches is that an HTTP connection protocol was used instead of a secure HTTPS protocol.

Some of the remaining vulnerabilities found are related to the use of outdated versions of application and database servers and personal computers, given that there were vulnerabilities of the software in its newer versions, where they have already been fixed.

The SRC's decision says that, given the volume, significance and sensitivity of the data at stake, the amount of the fine appears to be highly understated, but the court has no power to increase it.

The decision is not final and could be appealed by the NRA.

What are the most relevant AI updates?

Concept for the development of artificial intelligence in Bulgaria until 2030

On 16 December 2020, the Council of Ministers adopted a concept for the development of artificial intelligence in Bulgaria until 2030.

The document offers a comprehensive vision for the development and use of artificial intelligence in Bulgaria. It is based on the European Commission's strategic and programming documents, which consider artificial intelligence as one of the main drivers of digital transformation in Europe.

The main objective of the concept is to unite efforts in the development and implementation of artificial intelligence systems by creating scientific, expert, business and management capacity. It is envisaged to provide a modern communication and scientific infrastructure for the development of digital technologies of a new generation. The education and lifelong learning system will be improved. It will support the development of research and the uptake of innovation in key sectors, as well as work will be done to put in place an ethical legal and regulatory framework that enjoys public trust.

Materials issues by the Bulgarian supervisory authority

The Bulgarian Commission for Personal Data Protection (CPDP) has issued materials related to the application of big data and artificial intelligence. Although non-binding in nature, the materials aim to support the practical implementation of the GDPR and to clarify some key issues in the processing personal data.

- Big data and related profiling capability (brochure for data controllers) – it outlines risks in the processing of large databases, including in training artificial intelligence (AI) devices, such as neural networks, and statistical models to predict certain events or behaviors, where often the training data is of questionable quality and not neutral;
- Contemporary threats and challenges to the protection of personal data in the context of trends in the development of artificial intelligence and new technologies for facial recognition – the material focuses on benefits of the development of artificial intelligence and new facial recognition technologies; risks from the use of artificial intelligence and new facial recognition technologies; requirements to be met by AI applications; recommendations on the use of artificial intelligence and new facial recognition technologies.

What are the most relevant upcoming data protection developments?

Finalization of the national legal framework in the area of accreditation

In its Annual Report for 2022 the Commission for Personal Data Protection (CPDP) outlined its objectives and priorities for 2023, among which the adoption of requirements for accreditation of certification bodies and for accreditation of bodies monitoring codes of conduct.

The abovementioned requirements could be adopted after final opinion by the European Data Protection Board (EDPB).

The EDPB has adopted Opinion 14/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 of the GDPR. The EDPB's conclusion was that the draft accreditation requirements of the Bulgarian supervisory authority may lead to an inconsistent application of the accreditation of monitoring bodies and the certain changes need to be made.

The adoption of the requirements for accreditation of certification bodies and for accreditation of bodies monitoring codes of conduct is still expected. This is a necessary step in order for the national legal framework in the area of accreditation to be finalized.

Employee data protection

On 20 November 2023, a Bill for amending and supplementing the Labor Code ("the Bill"), concerning the legal framework for remote work, was submitted to the National Assembly.

Part of the changes are related to the regulation of requirements for the use of information systems by the employer for assigning and reporting the work, including regarding the implementation of systems for algorithmic management of work processes (and so-called artificial intelligence). The Bill introduces requirements for providing information to employees when using such systems, as well as the possibility to request a human review of the automated decisions made when they affect the rights of employees.

Denmark

Contacts

Jeanette Vallat

Partner, Deloitte Legal Denmark

jvallat@deloitte.dk

Simone Mai Petersen

Senior Consultant, Deloitte Legal Denmark

smpetersen@deloitte.dk

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

Disclaimer: Deloitte Statsautoriseret Revisionspartnerselskab disclaim any and all liability for the content provided to you and your use hereof.

The Danish Data Protection Agency has introduced a catalogue with an overview of different examples of precautionary measures

"According to GDPR, data controllers must ensure appropriate technical and organizational measures - this is very general, but the catalogue is an attempt to make it concrete and usable,"

"Many of the measures contain concrete examples based on the Danish Data Protection Agency's experience from supervision, notified breaches of personal data security, EDPB's guidelines and applicable ISO standards. In addition, many of the measures also provide links to specific relevant decisions in this area. These can be found under each measure in a box called "Practice"."

Hotel group sentenced to pay fine of DKK million

"The infringement consisted in the hotel group failing to comply with the deletion deadlines it had itself set. The Danish Data Protection Agency estimated that approximately 500,000 customer profiles should have been deleted at the time of the inspection visit. The erasure of personal data that is no longer necessary to store, is one of the fundamental principles of data protection rules, as at the same time the risk of misuse of such data is limited."

The decision will most likely set a precedent for the estimation of similar fines.

New guidelines from the Danish Data Protection Agency regarding managing of user access/rights

"Managing user access is a basic part of information security, but it can cause practical issues. In case of challenges with access rights, there is an increased risk of a wide range of breaches of personal data security - from unauthorized access by employees to abuse from former employees to targeted hacker and ransomware attacks from outside."

In the guidelines, the concept of rights management is used as an overarching concept, which includes managing access to the organization's IT systems and premises, as well as the extent of the data the individual users have access to. The guidelines seek to shed light on the threats that are known from the Data Protection Agency's own case complex and from the news media. The guidelines can help data controllers and processors to take the necessary precautions and security measures in their work with data protection compliance.

Hospital could not use consent to publish photos of patients on Instagram

The Danish Data Protection Agency has, at its own initiative, assessed that the publication of personal data regarding patients cannot be carried out in compliance with data protection regulation.

"After further investigation, the Danish Data Protection Agency found that the hospital cannot use consent as a legal basis for processing, as there is an unequal relationship between the patient and the hospital. On this basis, the Danish Data Protection Agency has issued an order to the hospital to delete posts containing health information (in the form of photos) about patients from the Instagram account within four weeks."

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

Disclaimer: Deloitte Statsautoriseret Revisionspartnerselskab disclaim any and all liability for the content provided to you and your use hereof.

Quote from the Danish Data Protection Agency (regarding AI):

"The Danish Data Protection Agency will continue to focus on the use of artificial intelligence. In the shorter term, the Agency will, among other things, prepare a template for carrying out impact assessments that authorities can use in their work with and usage of AI. In the slightly longer term, the Danish Data Protection Agency will look at more guidance on how organizations can handle the risks that may be associated with the use of AI, such as bias and lack of transparency."

More material including guidelines etc. can be expected from the Danish Data Protection Agency.

What are the most relevant AI updates?

Disclaimer: Deloitte Statsautoriseret Revisionspartnerselskab disclaim any and all liability for the content provided to you and your use hereof.

New guidance on public authorities' use of AI and mapping of AI across the public sector

In the guidelines, the Danish Data Protection Agency takes a closer look at artificial intelligence and the basic considerations that authorities must make before they start developing AI solutions. This includes, among other things, questions about the basis for processing, the obligation to provide information and impact assessment.

"In addition to the new guidelines, the Danish Data Protection Agency has mapped public authorities' use of AI. The mapping of the use of artificial intelligence in the public sector provides the clearest insight to date into public authorities' use of artificial intelligence solutions and their data protection law considerations in this regard. Among other things, the survey shows that the use of artificial intelligence is not yet widespread among public authorities. To the extent that artificial intelligence solutions are used in the public sector, they are often standard solutions, or the same specially developed solution used by several authorities."

France

Contacts

Hervé Gabadou

Partner, Deloitte Legal France

hgabadou@avocats.deloitte.fr

Tony Baudot

Senior Manager, Deloitte Legal France

tbaudot@avocats.deloitte.fr

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

The French National Commission for Information Technology and Civil Liberties (CNIL) focused on four main areas for its controls in 2023 in France:

The use of “smart” cameras by public entities

The development of so-called “enhanced” or “smart” cameras, mainly by local authorities, is a recurring subject of complaints to the CNIL. The use of these devices is mostly scheduled for large-scale sporting events taking place in 2023 (Rugby World Cup) and 2024 (Olympic Games).

The CNIL has made the use of "enhanced" cameras a priority in its 2022-2024 strategy which has led to the implementation of a series of actions that include support for private and public entities, as well as controls. For example, after conducting a public consultation in which it expressed its stance on this type of technology, the CNIL has decided to consider this subject as a priority for its audits in 2023. This enables the CNIL to verify that public players are complying with the legal framework.

Access to digital patient records in healthcare sector establishments

Over the past few years, the CNIL and the French Ministry of Health have exchanged views on health data protection, such as on the General Security Policy for Health Information Systems (PGSSI-S), the shared medical record (DMP), the health professionals' card (CPS-eCPS), and the "pro Santé connect" service. These systems have been subject to requests for opinions and advice. Health data protection is a recurring issue which concerns all healthcare establishments.

The CNIL has already initiated checks on access to computerized patient records in 2022 and continued to do so in 2023. This decision was taken in response to complaints received by the CNIL alleging unauthorized third-party access to computerized patient records in healthcare establishments. Inspections also examine all measures put in place to ensure data security.

The use of the FICP (database records for credit repayment incidents)

The *Banque de France*’s FICP database is a record of information on payment incidents linked to personal credit overdrafts and loans granted for personal purposes, as well as information on cases of excessive indebtedness. It is mandatory for banks to consult this database, especially before granting a credit.

Entries in this file are therefore particularly important, as they can hinder individuals in their subsequent dealings with banks. The accuracy of the data contained in the file, its retention period and compliance with the conditions governing its management are therefore crucial. Controls focus on the conditions under which banks access the file, extract information from it and update it after payment incidents have been cleared.

User tracking by mobile applications

Phone manufacturers provide app publishers with identifiers enabling users to be tracked for advertising, statistical or technical purposes (Apple IDFA, IDFV, Google AAID, etc.). The systematic use of these identifiers, the "smartphone" equivalent of the massive use of cookies on websites, is often carried out without the information or consent of users.

Following the amendment of the recommendation on the use of cookies and other trackers, several checks have already been carried out on applications that access identifiers generated by mobile operating systems in the absence of user consent. The CNIL has continued to focus on controlling this in 2023.

What are the most relevant data protection updates?

Data protection laws and regulations, guidelines

The CNIL has not adopted new data protection laws in 2023 but has published new guidelines such as regarding artificial intelligence (see hereafter), the transfer of data in the context of APIs, the health sector, the sport and education sector and has updated its guidelines on the security of personal data. The CNIL has also adopted several important decisions and sanctions concerning GDPR compliance.

The CNIL published a series of questions & answers on its website, regarding the adequacy decision for safe and trusted EU-US data flows adopted by the European Commission on 10 July 2023.

Health sector

- The CNIL published guidelines and a practical information sheet on retention periods in the social and medico-social sector.
- The CNIL has adopted two reference methodologies for accessing the main National Health System (SNDS) database in the context of health research.
- The CNIL and the French National Pharmacists Association published a guide to help pharmacists comply with data protection regulations. The CNIL and the French National Doctors Association entered into a partnership towards health data protection.
- The CNIL highlighted its concerns for data protection in the context of the merger of the Health insurance card (*Carte Vitale*) and the identity card, and the creation of a e-health insurance card.
- The CNIL initiated a public consultation on the use of surveillance cameras in nursing homes.

Sport and education sector

- The CNIL published its first two practical information sheets related to the sport sector to help players in the sports ecosystem to comply with the GDPR.
- The first sheet deals with criminal record checks for professionals, volunteers and other people involved in sports organizations (instructors, athletes, medical staff, judges and referees, accompanying parents, etc.).
- The second sheet sets out the rules on the length of time personal data can be kept and suggests a methodology for defining a consistent and appropriate period.
- The CNIL published a recommendation for the remote monitoring of online examinations.

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

Recent cases

16 March 2023: The CNIL imposed an administrative fine of €125,000 on a scooter rental company for, among other things, disproportionately infringing its customers' privacy by geolocating them on an almost permanent basis. This decision was in line with the CNIL's focus on priority areas of everyday concern to the French population, including geolocation for local services.

15 June 2023: The CNIL fined online advertising company €40 million, notably for failing to verify that the people whose data it processes have given their consent. Following complaints filed by the associations Privacy International and None of Your Business, the CNIL carried out several inspections at the advertising company. During its investigations, the CNIL identified several breaches concerning the lack of proof of people's consent to the processing of their data, information and transparency, and respect for individual rights.

18 September 2023: The CNIL fined an air freight company €200,000 for collecting too much data from its employees, violating their privacy and failing to cooperate sufficiently with the CNIL's departments.

12 October 2023: The CNIL fined a French mass media company €600,000, notably for failing to comply with its obligations in terms of commercial prospecting and individual rights.

7 November 2023: The CNIL issues 10 new fines under its simplified procedure for a total of €97,000. In these 10 decisions, two matters stood out: geolocation of company vehicles and video surveillance of employees.

Firstly, the CNIL points out that the ongoing recording of geolocation data, with no possibility for employees to stop or suspend the system during their breaks, is, unless there is special justification, an excessive infringement of employees' freedom of movement and right to privacy.

Secondly, it reaffirms its position on the use of video surveillance systems that constantly film employees at their workstations for no specific reason. Indeed, the prevention of accidents in the workplace and the gathering of evidence do not justify the implementation of continuous video surveillance of workstations. Under these conditions, the personal data obtained from the video surveillance system is neither adequate nor relevant. The permanent surveillance of employees is, with a few exceptions, disproportionate to the purposes being pursued.

What are the most relevant AI updates?

Creation of a new department dedicated to artificial intelligence within the CNIL

For several years now, the CNIL has been working to anticipate and respond to the issues raised by AI. Its new Artificial Intelligence Department, created in January 2023, is dedicated to these issues, and supports the CNIL's other departments, which are also faced with the use of these algorithms in many contexts.

The Artificial Intelligence Department created within the CNIL will have a staff of five people and will be made up of specialist lawyers and engineers.

The main tasks of the Artificial Intelligence Department is to:

- Make it easier for the CNIL to understand how AI systems work, but also for professionals and individuals;
- Consolidate the CNIL's expertise in understanding and preventing privacy risks associated with the use of these systems;
- Prepare for the entry into force of the European regulation on AI (currently under discussion at European level); and
- Develop relations with players in the ecosystem.

In 2023, the CNIL extended its work on “smart” cameras and broadened its focus to include Generative AI, large-scale language models and derivative applications (in particular chatbots). Specific work on datasets for AI was also launched.

The CNIL’s action plan for artificial intelligence

The CNIL’s action plan is based around four areas:

- **Understanding how AI systems work and their impact on people**. Indeed, these new techniques raise questions for data protection such as the loyalty and transparency of data processing underlying the functioning of AI models, the protection of publicly accessible data, the protection against bias and discriminations, security challenges, etc.
- **Enabling and supervising the development of AI systems that respects privacy** through the CNIL’s first application sheets on AI published in 2022, a guide for professionals, the CNIL’s position on “smart” surveillance cameras, etc.
- **Bringing together and supporting innovative players in the AI ecosystem in France and in Europe**. The CNIL has launched different programs to support innovative players such as a specific support programme for suppliers of “smart" video surveillance as part of the experiment provided for by the law relating to the 2024 Olympic and Paralympic Games.
- **Auditing and controlling AI systems and protecting individuals.** In 2023, the CNIL's supervisory action focused on: compliance with the position on the use of “smart" video surveillance, the use of artificial intelligence in the fight against fraud, and investigating complaints lodged with the CNIL.

This work will also help prepare for the implementation of the draft European AI regulation, currently under discussion.

What are the most relevant AI updates?

AI "how-to" sheets published by the CNIL

In publishing these "how-to" sheets, the CNIL wishes to provide practical clarifications and recommendations for the development of AI systems and the creation of datasets involving personal data used for their learning. The CNIL indicates that the main French players in the AI field have raised a strong **need for legal certainty**.

The "how-to" sheets concern only the development phase where the processing of personal data is involved (and **subject to the GDPR**) and do not deal with the deployment phase.

They are organized in nine documents divided as follows:

- The introduction specifies the scope of the how-to sheets;
- Sheet 1 deals with the legal regime applicable to data processing in the development phase of the AI system;
- Sheet 2 deals with the determination of the purpose of the data processing for the creation of a dataset for the development of an AI system;
- Sheet 3 refers to the legal qualification of AI system providers;
- Sheet 4 sets out how to choose the legal basis for the processing and the additional checks to be carried out according to the method of collection or in the case of re-use of the data;
- Sheet 5 deals with the carrying out of a data protection impact assessment; and
- Sheets 6 and 7 help stakeholders to take data protection into account in the design choices of the AI system and in the data collection and management. A documentation model is provided in the annex of Sheet 7.

First answers from the CNIL for innovative and privacy-friendly AI

By submitting for public consultation its first how-to sheets on the creation of datasets for the development of artificial intelligence systems, the CNIL confirmed the compatibility of AI research and development with the GDPR, provided that it does not cross certain red lines and respects certain conditions.

The purpose limitation principle also applies appropriately to general purpose AI (GPAI) systems. This principle requires the use of personal data only for a specific goal defined in advance. Regarding AI, the CNIL recognizes that all future applications cannot be defined at the training stage, provided that the type of system and the main possible functionalities have been well defined.

The principle of data minimization does not prevent the use of large datasets. However, the data used must, in principle, have been selected to optimize the training of the algorithm while avoiding the use of unnecessary personal data. In any case, certain precautions to ensure data security are essential.

The retention period of training data may be long if justified. Training datasets may need longer retention periods as they require significant scientific and financial investment and sometimes become standards widely used by the community.

Re-use of datasets is possible in many cases. Finally, the CNIL considers that the re-use of datasets, in particular publicly available data on the Internet, is possible to train AI systems, provided that the data has not been collected in a manifestly unlawful manner and that the purpose of re-use is compatible with the initial collection. In this regard, the CNIL considers that the provisions on research and innovation in the GDPR provide a regime for innovative AI actors who use third-party data.

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

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

- **Objective 1: Promote the control and respect of the rights of individuals.** This implies providing individuals with the proper tools and information enabling them to understand and exercise their rights. The CNIL's actions should be carried out in partnership with the European community to drive change in the practices of major industry players and set new standards.
- **Objective 2: Promote the GDPR as a confidence-building tool for data controllers.** As data protection has gradually become an essential part of the daily culture of data controllers, the CNIL will be further enhancing its support services by making the legal framework easier and more foreseeable, developing compliance tools, and helping data controllers prevent cybersecurity threats.
- **Objective 3: Prioritize targeted regulatory actions on topics of high privacy concern.** The CNIL will implement a general action plan around three key topics: "smart" cameras, cloud computing and personal data storage in smartphone apps. It will start its compliance strategy with a doctrine-setting phase. The second phase will include the development of practical compliance within the concerned sector. Finally, the CNIL will conduct control operations and, if necessary, adopt corrective measures.

Furthermore, the CNIL has initiated public consultations in 2023:

- **Security of high-risk IT systems in case of personal data breach.** The CNIL initiated a public consultation on a draft recommendation to provide the best possible support for the concerned parties. For processing operations presenting significant risks, the CNIL wishes to gather all the advanced security practices it recommends in a single document. This consultation was closed on 22 October 2023. The CNIL will **publish the final version of the recommendation in early 2024.**
- **Artificial intelligence.** The CNIL has initiated a public consultation regarding the creation of datasets for AI. The public is invited to comment on the first "how-to" sheets published by the CNIL regarding the creation of datasets for the development of artificial intelligence systems. This public consultation is opened until 15 December 2023. The contributions will be analyzed at the end of the public consultation to allow the **publication of the final "how-to" sheets on the CNIL website in early 2024.**

Germany

Contacts

Nikola Werry

Partner, Deloitte Legal Germany

nwerry@deloitte.de

Dr. Till Contzen

Partner, Deloitte Legal Germany

tcontzen@deloitte.de

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

Data protection laws and regulations:

Whistleblower Protection Act (HinSchG)

On 2 July 2023, the new German Whistleblower Protection Act (abbreviated in German to "HinSchG") came into force. It is the German implementation of the EU Whistleblowing Directive (Directive (EU) 2019/1937). The aim of the act is to create legal certainty for whistleblowers who help to uncover and punish wrongdoing through their reports. § 2 HinSchG is broadly defined. Whistleblowers enjoy the protection of the law, among other things, when reporting violations of criminal regulations or statements made by public officials that violate the duty of loyalty to the constitution.

Companies and organizations with more than 249 employees must set up and operate a whistleblower system since the effective date. As from 17 December 2023, this obligation will also apply to companies with at least 50 employees.

Health Data Utilization Act (GDNG)

The draft of the Health Data Utilization Act (abbreviated in German to "GDNG") was adopted in August 2023 and is now being discussed in the federal parliament. The law serves to implement the digitalization of healthcare and nursing care. The aim is to make it easier to use health data for public welfare purposes. A decentralized health data infrastructure with a *central data access and coordination point* for the use of health data will be established for this purpose.

This will break down bureaucratic barriers and facilitate access to research data. For the first time, data from various sources will be able to be linked together, for instance information from the Research Data Center and the Cancer Registry. The data is linked via a technical process. In this procedure, respective pseudonyms of the sources are collected in a protected manner and common research identification numbers are generated for each event. The pseudonyms are not disclosed to the users of the data.

What are the most relevant data protection updates?

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

Data Protection Conference ("DSK"):

- **24 November 2022:** Application notes on the standard data protection model. The model represents a method for data protection consulting and auditing on the basis of standardized performance targets.
- **29 November 2022:** Decision on the impact of the new consumer protection regulations on digital products in the German Civil Code on data protection law.
- **5 December 2022:** Guidance from the supervisory authorities for telemedia providers from 1 December 2021. The guideline covers the following issues: the new legal situation for telemedia as of 1 December 2021, the protection of privacy in end facility according to § 25 Telecommunications-Telemedia Data Protection Act (abbreviated in German to “TTDSG”) and the lawfulness of processing according to GDPR.
- **31 January 2023:** Decision on the data protection assessment of access to personal data by public authorities of third countries.
- **11 May 2023:** Decision on the data protection assessment of access to personal data by public authorities of third countries .The resolution is based on the judgment of the CJEU of 30 March 2023, on the requirements for an implementation of the employee data protection law.
- **4 September 2023:** Application instructions to the EU-US Data Privacy Framework. The instructions are aimed at both data controllers and processors in Germany who transfer personal data to the US. They are further aimed at affected people.
- **17 October 2023:** Resolution on the planned chat control of the EU Commission. The aim of the monitoring is to prevent and uncover child abuse on the Internet. The DSK points out that due to the selection of the means of control, in some cases very sensitive information of all users who exchange e-mails or other messages in online services are affected by monitoring without distinction and regardless of suspicion.

What are the most relevant data protection updates?

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

States Supervisory Authority:

Bayern

- Bavarian public authorities and the Windows telemetry component: The Bavarian Commissioner for Data Protection sheds light on the uncertainty that comes with using Microsoft Windows. The possibility exists that Windows itself can transmit personal data to the manufacturer, among other things.

Berlin

- On 31 May 2023, the Berlin Commissioner for Data Protection and Freedom of Information imposed a fine of €300,000 on a bank for lack of transparency regarding an automated individual decision. The bank had refused to provide a customer with comprehensible information about the reasons for the automated rejection of a credit card application.
- The Commissioner further imposed a fine of €215,000 against a Berlin-based company for unlawful processing of personal data on employees during their probationary period.

Hamburg

- Guidance on handling data breach notifications according to Art. 33 GDPR: The Hamburg Commissioner for Data Protection and Freedom of Information provides a detailed guidance explaining how to report data breaches. What is at stake, which cases are to be reported, what are the deadlines, how to report.

What are the most relevant data protection updates?

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

States Supervisory Authority:

Niedersachsen

- Handout: Data protection compliant consent on websites - requirements for consent layers
- FAQ on commissioned processing under article 28 of the GDPR

Nordrhein-Westfalen (NRW)

- Guide on the response to a cyberattack: The guide covers the most relevant first steps to take in the event of a cyberattack. The Commissioner further imposed a fine of €215,000 against a Berlin-based company for unlawful processing of personal data on employees during their probationary period.
- NRW state data protection commissioner can fine employees of public bodies: If employees of public bodies process official data for private purposes, they can be sanctioned by the state data protection commissioner. This applies both to employees of public agencies of the state and municipalities in NRW and to employees of federal authorities who live in NRW.

Rheinland - Pfalz

- On 24 April 2023 the State Commissioner for Data Protection and Freedom of Information of Rhineland-Palatinate has sent a catalogue of questions to the operator of ChatGPT, OpenAI. Among other things, it deals with questions about the legal basis for the data that ChatGPT processes, the protection of children's data and information about the processing.

What are the most relevant AI updates?

Federal government: the GDPR applies to ChatGPT

A parliamentary group has submitted a small inquiry to the federal government which contained 17 questions on the subject of ChatGPT and data protection. The background to the request is the one-month ChatGPT ban by Italy. The questions included the legality of the GDPR, the legal basis for blocking ChatGPT in Germany and the dangers of integrating ChatGPT into Microsoft products such as Office and Teams. The federal government replied that the processing of personal data by OpenAI, the company operating the ChatGPT, is subject to the provisions of the GDPR and the German Federal Data Protection Act (BDSG). The competent independent data protection supervisory authorities are responsible for deciding whether and, if so, which measures are taken against the company operating OpenAI ChatGPT. They are granted corresponding powers in the GDPR.

In April 2023, the "AI Taskforce of the Data Protection Conference" took over the topic of data protection and ChatGPT. The data protection authorities of the federal states are reviewing the compatibility of ChatGPT with the GDPR and are trying to obtain more detailed information from Italy about the blocking of ChatGPT. The outcome of the review is still pending.

First agreement on protection against AI

On 26 November 2023, together with 17 other countries, Germany has signed an international agreement to protect people against misuse of artificial intelligence. Among the 17 countries were the US, Israel, Singapore and Nigeria. The agreement is the latest initiative in a series of attempts by governments around the world to exert more influence on the international development of AI. However, the agreement is non-binding and mainly contains general recommendations, such as monitoring AI systems for misuse, protecting data from manipulation and checking software providers.

Regarding the EU AI Act, Germany, France and Italy agreed on a position paper on its regulatory content. The proposal provides for mandatory self-regulation for AI providers in the EU, in which companies can voluntarily adhere to certain rules. Currently the EU AI Act is in the trilogue process.

What are the most relevant upcoming data protection developments?

Draft law for a new Federal Data Protection Act (BDSG-E)

The aim of the new draft law is to take up the agreements of the coalition agreement 2021-2025 of the current government in Germany as well as to implement results that have emerged from the evaluation of the Federal Data Protection Act (abbreviated in German to “BDSG”).

Among other things, video surveillance of publicly accessible spaces by non-public bodies is to be restricted. Video surveillance is to be permitted if it is necessary for the tasks as well as for the enforcement of the house right and only if interests worthy of protection of those concerned do not prevail. In accordance with § 16a of the draft law, the Data Protection Conference is to be institutionalized in the Federal Data Protection Act. The aim of the Data Protection Conference is to uphold and protect fundamental data protection rights, to achieve uniform application of European and national data protection law, and to work together to promote its further development.

Despite the significant progress, the draft meets with legal concerns, which is why the development of the draft must continue to be monitored.

Mobility data protection law

A mobility data law is planned to ensure the free accessibility of traffic data. Transport companies and mobility providers are to provide their real-time data under fair conditions. The law regulates who will be obliged to provide the data in future and how access to the data will be granted. In particular, the law is intended to contribute to the availability of more and better travel and transport infrastructure data. In July 2023, the Federal Ministry for Digital and Transport presented a key issues paper. A draft bill on the Mobility Data Act is to be presented by the end of 2023.

Employee data protection

In March 2023, the ECJ issued a ruling on § 23(1) sentence 1 of the Hessian Data Protection and Information Security Act (abbreviated in German to “HDSIG”), according to which the regulation is not covered by the opening clause of article 88(1) of the GDPR and is therefore invalid. This concerns data processing for the purposes of the employment relationship. Due to the almost identical wording of § 23(1) sentence 1 HDSIG with § 26 of the BDSG, the question now arises as to whether the federal provision is also invalid. The Federal Ministries of Labor and Social Affairs and of the Interior and Home Affairs have presented a key issues paper on the innovation of the BDSG and especially on data protection for employees. There could be some changes here in 2024.

Greece

Contacts

Apostolos Vorras

Partner, KBVL Law Firm,
Deloitte Legal Greece

avorras@kbvl.gr

Fay Mantzouni

Associate KBVL Law Firm,
Deloitte Legal Greece

fmantzouni@kbvl.gr

What are the most relevant data protection updates?

Recent guidelines

Guidelines 1/2023 on the processing of personal data for the purpose of communication of political nature

The Hellenic Data Protection Authority (HDPA) has issued guidelines requiring political organizations, including parties, MPs, MEPs, and their factions, to comply with GDPR. These entities are considered data controllers when they process the personal data of individuals for the purpose of promoting political ideologies and influencing political behavior, whether before or during electoral campaigns. The guidelines include both illustrative examples of lawful personal data processing for political communication and highlight practices that contravene data protection laws. Furthermore, the HDPA specifies that it is permissible for politicians to employ messaging applications of the 'Information Society' for political communication, provided they do so within the legal framework.

Investigations into the use of spyware

In late July 2022, the HDPA launched an investigation into the use of "Predator" spyware in Greece. This was in response to reports from five individuals. The HDPA's authority comes from GDPR and e-privacy laws protecting personal data in electronic services. The investigation revealed attempts to install spyware via misleading SMS links sent to numerous mobile users. The HDPA took various actions, including issuing orders, conducting checks, collecting information, and imposing fines. Over 350 related SMS messages were found, with more than 220 containing deceptive links. Notifications were sent to 92 phone numbers that received these messages. The investigation is still in progress.

What are the most relevant data protection updates?

30/2023

The Hellenic Data Protection Authority (HDPA) conducted an extraordinary on-site inspection of the Athens Urban Transport Organization (OASA) regarding the protection of personal data processed within the automatic fare collection system, also known as the "electronic ticket" system. The HDPA found that OASA retained data for 20 years without justification, violating storage limits, had an insufficient DPIA, lacking clarity on data retention purposes, risks were not addressed per privacy by design principles and processing purposes were ambiguously stated. Consequently, the HDPA imposed a fine of €50,000 on OASA for violating article 5(1)(e), article 25(1) and article 35(1) of the GDPR, and ordered compliance regarding the determination of data retention periods for various processing purposes and the revision of the impact assessment concerning personal data.

25/2023

The HDPA found that a credit institution processed personal data of a complainant and approximately 20,000 customers unlawfully, violating data processing legality and failing to implement necessary measures to process only data needed for specific purposes. The credit institution had erroneously notified certain customers about the transfer of their personal data to debt management firms, despite these individuals not having any outstanding loans, thereby lacking a legal basis for such processing. While no actual data transfers to the asset management company were evidenced, the HDPA retains the authority to address this issue in the future. Consequently, the credit institution was penalized with administrative fines totaling €210,000 for infringing upon article 5(1)(a), article 6, article 25(1), and article 15(1) of the GDPR.

20/2023

The HDPA investigated complaints from a subscriber to a telecommunication service provider. Those complaints related to its practice of repeatedly sending promotional messages to the subscriber, despite opposition and repeated protests, and failure to satisfy his access rights requests. Fines imposed include €60,000 for violating article 21(3) of the GDPR due to sending five promotional messages against the subscriber's wishes and delisting their phone number without consent for three months, €60,000 for not satisfying access rights, not providing even a negative response, and hindering the exercise of access rights under false pretenses of identification issues, and €30,000 for violating article 25(1) of the GDPR due to lacking necessary procedures to ensure the right to object and stop data processing for promotional purposes.

2/2023

The HDPA fined computer design company €50,000 for non-cooperation during an investigation. Since July 2022, the HDPA has been probing the installation of spyware on mobile devices to secretly monitor users and collect personal data. An administrative check on the company began in September 2022 with on-site inspections. The company unjustifiably delayed responding to the HDPA's inquiries and refused to provide information it undoubtedly possessed, violating article 31 of the GDPR, which mandates cooperation with the supervisory authority. Additionally, the HDPA ordered the company to immediately provide specific information necessary for the investigation. The probe into the company and the use of spyware within Greece continues, with the HDPA gathering evidence from various entities inside and outside Greece and the EU.

What are the most relevant **AI updates**?

Greek Law No. 4961/2022 on emerging information and communication technologies, enhancement of digital governance, and other provisions

Greek Law No. 4961/2022 sets regulations for AI in public and private sectors, focusing on safe development and use, while promoting digital governance. It mandates obligations for entities producing, distributing, exploiting, and making use of advanced technologies and especially AI, ensuring individual and entity protection. Objective of this law is to prepare the legal ground for a schemeless implementation of the anticipated EU AI Act that is expected to be adopted within the first months of 2024.

Law No. 4961/2022 touches upon issues relating to artificial intelligence (AI), the internet of things (IoT), the provision of postal services using unmanned aircraft systems (UAS), distributed ledger technologies (DLT) and smart contracts.

The law provides for several obligations that apply either to the public or/and the private sector including the obligation:

- To execute AI impact assessment;
- To provide public information about the operating parameters of the AI system, as well as about the decisions that are made or supported through it;
- To maintain a registry of the AI systems;
- To provide information to employees about the use of an AI system which will have an impact on working conditions, selection, hiring, or their evaluation; and
- To adopt a policy of ethical use of data, which includes information about the measures and procedures it implements during the use of AI systems.

What are the most relevant upcoming data protection developments?

Legislative proposal for the establishment of a National Cybersecurity Authority

The Greek Council of Ministers has introduced a draft legislative act for the establishment of an independent National Cybersecurity Authority that will assume the role of the national supervisor for cybersecurity issues and will be supervised by the Minister of Digital Governance. The aim pursued is the effective prevention and management of cyberattacks, as well as the development of the cybersecurity ecosystem in Greece.

The establishment of the Authority will address certain pressing issues and more specifically:

- The need to transpose Directive NIS2 that requires the further widening of the applicability scope and the increase of the supervised entities;
- Ensuring the trust of citizens and businesses in digital services;
- Institutional and technological fortification against cyber threats and overall enhancement of the level of cybersecurity in the country;
- Promoting investments in the field of cybersecurity, as well as strengthening the ability to draw European funds;
- Enhancing the ecosystem of digital innovation; and
- Promoting education and awareness on cybersecurity issues, as well as upgrading digital skills in cybersecurity.

The powers of the National Cybersecurity Authority will include, *inter alia:*

- The coordination, design and implementation of the National Cybersecurity Strategy in cooperation with other competent authorities; and
- The supervision of the entities falling within the NIS2 scope.

The proposal constitutes a significant step towards responding to the increasing national needs and the pressing Union commitments, upgrading the level of supervision, information, and support of the involved entities in the field of cybersecurity, shaping an environment with secure infrastructures.

Digital Transformation Bible

The Greek government has introduced a comprehensive digital transformation program, also known as the Digital Transformation Bible. Recognizing the positive outcomes of the implementation of digital practices in the private sector, the government launched this initiative in 2020, as part of a long-term strategy to digitize all public sector services offered to businesses until 2025. The main objective is to streamline processes digitally, thereby reducing the administrative burden on businesses. Indicatively, this project involves the development of public information systems that support B2B, B2G, B2C transaction processes, especially regarding GEMI, AADE, EFKA, Ergani, OAED, First Instance Courts, and 'NotifyBusiness', all of which facilitate the establishment, licensing, transfer, and oversight of business operations through secure and verifiable digital transactions. Looking forward, we can expect the launch of additional digital initiatives aimed at further streamlining public services.

Italy

Contacts

Ida Palombella

Partner, Deloitte Legal Italy

ipalombella@deloitte.it

Pietro Boccaccini

Director, Deloitte Legal Italy

pboccaccini@deloitte.it

What are the most relevant data protection updates?

Transparency Decree: transparent working conditions

Starting in August 2022, employers in Italy are now required to provide their employees or workers with more transparent information (Legislative Decree No. 104/2022) about any automated decision-making or monitoring systems that are used to make decisions about their employment, such as hiring, assigning tasks, giving raises or terminating their contract. This applies to all forms of employment and working contracts.

In May 2023, the so-called Labor Decree stated that the transparency obligation only applies to fully automated systems, that is to say systems that make decisions without any human input.

In light of these new rules employers shall, among other obligations:

- Map the tools used in the employment context and carry out specific assessments on the use of fully automated systems;
- Carry out data protection impact assessment and implement stronger safeguards for protecting personal data, based on the possible risks for the employees; and
- Strengthen the information they provide to individuals about how their personal data is being used through the relevant tools.

Whistleblowing Legislative Decree and guidelines on the implementation of such decree

In March 2023, Italy implemented the EU Whistleblowing Directive through Legislative Decree No. 24/2023.

The main peculiarities of the Italian legislation are the following: (i) a data protection impact assessment (DPIA) is mandatory before starting the relevant data processing activities; (ii) personal data should only be handled by authorized and trained individuals; (iii) whistleblowing reports, both internal and external, and the respective documents must be stored for the appropriate time to address the issue and, in any case, for no longer than five years from the outcome of the completion of the investigations; and (iv) in the context of groups, companies sharing whistleblowing resources and managing together whistleblowing reports, should consider themselves joint controllers and enter into a specific agreement.

In July 2023, the Italian Anticorruption Authority (ANAC) issued guidelines to clarify the interpretation of the Whistleblowing Decree, providing more detailed guidance.

For compliance with this law, organizations need to establish a whistleblowing mechanism to report potential breaches. In addition to the other compliance activities indicated above, companies should also implement appropriate anonymization measures, inform data subjects about the relevant data processing activities, regulate the relationship with any external provider (e.g., the supplier of the platform to manage the reports).

What are the most relevant data protection updates?

Code of conduct on telemarketing and tele sales

The Italian Data Protection Authority (Garante) approved a new code of conduct to protect individuals from aggressive telemarketing and tele sales activities. The code applies to the promoting or selling of goods and services directly to individuals in Italy through outbound phone calls.

The code of conduct aims to promote practices that ensure the protection of the individuals' rights to privacy and the processing in compliance with the privacy laws. In particular, it requires companies to:

- Identify an adequate legal basis for processing personal data;
- Appropriately inform data subjects about the processing;
- Conduct due diligence in the selection of commercial partners;
- Establish procedures for the exercise of data subjects' rights and data breach management;
- Provide detailed reports of their calling activities;
- Register the names of any person contacted who objects to the processing of their personal data, requests the erasure of the data or withdraws consent (within 24 hours); and
- Observe "quiet hours".

The code also prohibits the use of data related to criminal convictions or crimes for advertising purposes.

In any event, the code allows for the processing of special categories of data, if collected in the context of specific contractual relationships with the data subjects and where their specific consent is collected.

Data broker fined for unlawful marketing practices

The Garante fined a data broker company €300,000 for engaging in unlawful marketing practices. Indeed, the company used a database to send promotional messages via SMS, email, and automated calls, which resulted in privacy infringements.

The Garante identified, among others, the following violations:

- Lack of transparency;
- Lack of legal basis for direct marketing purposes;
- Incorrect data qualification; and
- Use of deceptive design patterns in the company's websites, misleading users into giving consent for marketing purposes and communication of their data to third parties, for their own marketing purposes.

What are the most relevant data protection updates?

Italy's Data Protection Authority fines luxury department store chain for data protection breaches

The Garante fined a high-end Italian department store chain €300,000 for failing to meet its data protection obligations. In particular, the company did not: (i) adequately protect customers' data; (ii) conduct a data protection impact assessment (DPIA) for profiling activities; and (iii) provide clear information about data retention periods for marketing and profiling purposes.

The Garante ordered the company to clearly indicate different retention periods for each purpose, also differentiating them by considering the type of products sold.

A large cosmetics chain in Italy fined €1.4 million for GDPR violations

The Garante fined a large cosmetics chain €1.4 million for violating various GDPR provisions, such as the requirement to: (i) obtain valid consent for direct marketing communications and profiling; and (ii) limit the storage of personal data. Indeed, firstly the sanctioned company failed to demonstrate that the customers had provided valid consent for direct marketing communications and profiling (in relation also to data obtained in the context of M&A transactions).

Secondly, the Garante found that a vast amount of the controller's database was construed of data retained indefinitely (or until customers withdrew consent), including information on customers who never activated or renewed their loyalty cards.

Decision for processing health data without adopting adequate anonymization techniques and for erroneous data protection qualification

In June 2023, the Garante fined a company collecting and analyzing health data, provided by general practitioners, for not anonymizing data properly.

The Garante found that the company did not remove enough information from the data to make it anonymous. Indeed, the controller's measures, simply replacing patient IDs with an encryption system or an irreversible hash code, did not qualify as appropriate anonymization.

The Garante also found that the responsibility for the anonymization of the data laid on the fined organization and not on the general practitioners who collected: therefore, the company had to be qualified as the data controller. This is because:

- The company was the one establishing the methods to carry out the anonymization procedure on the data; and
- The purpose for such anonymization was to allow the company to carry out scientific research.

Finding that the company had erroneously considered to be processing anonymous data, another violation concerned the transparency principle, given that the patients were not provided with appropriate information about how their data was being used.

What are the most relevant AI updates?

Decalogue for the development of national healthcare services using artificial intelligence systems

On 10 October 2023, the Garante published a guide for the ethical development and use of artificial intelligence (AI) in healthcare (the Decalogue).The Decalogue outlines the key principles that should be followed when using AI in healthcare but serves as a valuable guideline applicable to any sector where AI systems are already in use or will be used in the future. The key aspects outlined in this document are:

- **Accountability**: The data controller must ensure that AI systems comply with privacy regulations and must be able to demonstrate the protection of data subjects' privacy rights;
- **Privacy by design and by default**: Data protection principles, starting from privacy by design and by default, must be integrated into the design and functioning of AI technologies;
- **Privacy roles**: A substantial approach should be followed in identifying the data controller and data processor;
- **Knowability**: The data subject has the right to know about the existence of decision-making processes based on automated processing and to receive meaningful information about the logic used;
- **Non-exclusivity of the algorithmic decision**: There must be human intervention in the decision-making process ("human in the loop");
- **Algorithmic non-discrimination principle**: The data controller should use reliable AI systems that reduce opacity and errors resulting from technological and/or human factors, periodically verifying their effectiveness through the implementation of appropriate technical and organizational measures;
- **Data protection impact assessment**: Processing carried out by AI systems might fall within "high risk" processing operations, for which a prior impact assessment (DPIA) is required, considering also consider specific AI-related risks (e.g., discrimination);
- **Integrity and confidentiality**: Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures;
- **Data quality**: The data controller must ensure that the data are accurate and - if necessary - updated, taking reasonable measures to promptly delete or rectify data that are incorrect in relation to the purposes for which they are processed;
- **Fairness and transparency**: Any information or communication relating to the processing of personal data should be concise, transparent, understandable, and easily accessible, using clear and plain language; and
- **Human supervision**: Human oversight should be based on highly qualified supervision to ensure the right not to be subject to a decision based solely on automated processing; such supervision should also occur during the algorithm training phase.

What are the most relevant AI updates?

Italian Supreme Court: understanding algorithms & reputational rating system is a key to valid consent

The Italian Supreme Court recently issued a ruling on the requirements for valid consent when using reputational rating systems.

The judgment arose from the appeal before the Court of Rome against the decision of the Garante prohibiting the processing of personal data by an association using a web platform capable of calculating - through the use of algorithms - the reputational rating of natural persons and legal entities.

The court found that for consent to be considered valid (freely given and informed), individuals must be able to understand the algorithm used to calculate the outcome or solve a particular problem; that should be described in a detailed manner and with an easily interpretable language.

Therefore, organizations that use AI systems must take steps to ensure that individuals are aware of the process that leads to the final score, providing clear and detailed explanations of how their algorithms work.

The Garante clamps down on an AI chatbot

The Garante imposed a temporary restriction on the data processing of an AI chatbot app. The app, equipped with a text and voice interface, allowed users to set up a virtual assistant that could be configured as a friend, partner or mentor.

The Garante pointed out that the app posed risks to children, as:

- It lacked an age verification mechanism;
- It served children with responses inappropriate for their age, including sexually inappropriate content; and
- It could affect children's mood, as the app's features aimed at improving users' emotional well-being, understanding their thoughts, calming anxiety, socializing and dating.

Moreover, the Garante found that:

- The app's data processing did not comply with transparency requirements; and
- It lacked a legal basis, considering that the performance of a contract could not be invoked as a legal ground, given that children are incapable to enter into a valid contract under Italian law.

What are the most relevant AI updates?

Proceedings against a Generative AI platform

During 2023, the Garante conducted a thorough investigation into a Generative AI platform processing personal data.

The Italian Supervisory Authority identified several shortcomings in the platform's compliance with data protection laws, prompting a temporary restriction on the processing of Italian users' personal data.

In particular, the investigation revealed that:

- The platform's age verification tools and child protection measures were inadequate; and
- The platform failed to comply with the obligations concerning legal basis for data processing, the rights of data subjects and the transparency of data processing activities.

The Garante also outlined specific measures the platform had to implement to lift the temporary limitations.

The Garante launched investigations into webscraping

The Garante launched an investigation to assess whether public and private websites in Italy are taking appropriate security measures to prevent the massive collection (so called "web scraping") of personal data for the training of AI algorithms by third parties.

The investigation focuses on all entities that:

- Operate as data controllers or provide services in Italy; and
- Make personal data publicly accessible online (including data that could be accessed by AI platforms using web scraping techniques).

The Garante's concerns stem from the growing practice of AI platforms to collect vast amounts of data, including personal information, from websites run by public and private entities through web scraping techniques. Information scraped includes personal data published for specific reasons (e.g., news, administrative transparency, etc.).

Following the investigation, the Garante may take necessary measures, even urgently.

What are the most relevant upcoming data protection developments?

The inspections of the Italian Supervisory Authority (Garante) – Inspection plan for second half of 2023

In the next months, the Garante is expected to issue decisions concerning the areas/sectors on which it has focused its inspection during the first half of 2023.

The Garante published its inspection plan for the second semester of 2023, focused on the following areas:

- Statistics and scientific research;
- Energy sector (in particular, the activation of unsolicited contracts and the performance of telemarketing activities);
- Biometric data through facial recognition (including in employment relationships);
- Processing of personal data by digital identity managers and service providers in the context of online services (also offered through apps);
- Correct implementation of the Garante's guidelines of 2021 on cookies and other tracking tools; and
- Other investigations against public and private subjects, to verify their compliance with the provisions on the protection of personal data, including investigations relating to complaints and formal alerts submitted to the Authority.

Codes of conduct

New codes of conduct are expected to be finalized soon, as the:

- Code of conduct concerning the processing by general practitioners and pediatricians; and
- Code of conduct concerning the processing by companies in the staffing industry.

Pay or consent cookie wall

In November 2022, the Garante opened an investigation into the use of cookie walls by some online newspapers and online businesses.

The Garante might take an official position in such regard in the upcoming months.

New guidelines on video-surveillance

The Garante is expected to issue new guidelines on the use of video-surveillance soon.

These guidance will provide an up-to-date overview on the laws applicable to video-surveillance, updating the 2010 decision.

The Netherlands

Contacts

Sebastiaan ter Wee

Partner, Deloitte Legal Netherlands

sterwee@deloitte.nl

Marlieke Bakker

Manager, Deloitte Legal Netherlands

mabakker@deloitte.nl

What are the most relevant data protection updates?

Dutch Data Protection Authority (DPA) (Autoriteit Persoonsgegevens)

Dutch DPA advises companies to be more transparent about privacy policies

The Dutch DPA advises large companies to be more transparent about how they handle personal data, for instance by paying consistent attention to privacy in their annual reports. The Dutch DPA has published two sets of guidelines; one guideline provides guidance on privacy in the annual report and the other guideline focuses on the role of the supervisory board, as their role also includes managing privacy risks. (December 2023)

Municipality fined

The Dutch DPA has fined a municipality €30,000 for keeping information about individual household waste longer than necessary and failing to properly inform residents about it. The municipality had replaced waste bins and underground containers with chipped versions linked to house addresses in 2018 and 2019 to promote waste separation. However, it kept the resulting data for longer than necessary for their purpose—until the bins were no longer in use or for five years for the tokens. The municipality has since reduced the data retention period to 14 days and sent a new letter, which it previously showed to AP, to inform residents. (November 2023)

GDPR certificate

The Dutch DPA has approved criteria that allow an institution to issue GDPR certificates. This brings a GDPR certification one step closer. As a result of this approval, the company “Brand Compliance” can continue its accreditation application with the Dutch Accreditation Council (RvA). Once Brand Compliance becomes accredited, it may issue GDPR certificates.

With a GDPR certificate, organizations can show their target audience that they process and protect personal data carefully. A GDPR certificate is not mandatory. (November 2023)

ISPS Privacy Code of Conduct approved

The Dutch DPA has granted approval to the Privacy Code of Conduct for Access Policy developed by ISPS companies and managed by Port Privacy B.V. ISPS companies are port businesses that handle international maritime traffic and are required to implement an access policy for safeguarding ships and port facilities, which involves personal data processing. The DPA has approved their code of conduct, but with a suspensive condition, due to the absence of a required supervisory body. The approval process of a code of conduct involves the DPA assessing whether it meets all the requirements of the General Data Protection Regulation (GDPR). The DPA's decision and the Privacy Code of Conduct for Access Policy for ISPS companies will be publicly accessible from 1 November 2023. (November 2023)

What are the most relevant data protection updates?

Dutch Data Protection Authority (DPA) (Autoriteit Persoonsgegevens)

Social media platform fined by Irish DPA, after initiated investigation by Dutch DPA

A social media platform, has been fined €345 million for violating the privacy of children in the EU and is required to make adjustments within three months, as announced by the Irish privacy watchdog on behalf of all EU regulators. The fine has been imposed for violations over five months in 2020. Aleid Wolfsen, Chairman of the Dutch Data Protection Authority, has described the violation as very serious, given the app's extensive use by children. The investigation was initiated by the Dutch regulator but was transferred when the company established its European headquarters in Ireland. (September 2023)

Dutch DPA initiates investigation into Dutch education executive agency

The Dutch DPA has started an investigation into an organization that provides student financing. The investigation follows the reporting about a potential discriminatory fraud detection system. (July 2023)

Data Breach Report 2022

In 2022, the Dutch DPA received 21,151 reports of data breaches as well as reports of 1,826 cyberattacks, with three large attacks exposing around 900,000 health care patients. Besides statistics, the report primarily educates the reader on how they can avoid being the victim of breached data, by instructing them to change their passwords and be alert for phishing. (June 2022)

Dutch social insurance bank fined

The Dutch DPA has fined a Dutch social insurance bank €150,000. The social insurance bank failed to properly identify callers to its call center, which allowed unauthorized persons to obtain personal data of recipients of an old-age pension (AOW). The social insurance bank has taken measures to prevent this from happening again in the future. (April 2023)

Car manufacturer urged to make cameras more privacy sensitive

Following an investigation by the Dutch DPA, a car manufacturer has made its in-car camera settings more privacy-friendly. When in a certain mode, the car films the surroundings of the car with built-in security cameras. The DPA's investigation concluded that the mode turned on too often and saved data for too long. The manufacturer has changed the settings so that the mode is turned off by default. When users turn the mode on for their car, it activates less frequently, and it only saves the recorded footage for 10 minutes. (February 2023)

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

Cookies

Dutch political parties place illegal cookies

Several political parties have been violating the Dutch Telecommunications Act by placing tracking cookies without the users' consent, according to an investigation by the Dutch Broadcasting Foundation (NOS). This allows the parties to later retarget visitors with personalized ads. The parties have acknowledged the error and are working on solutions. The Dutch DPA expressed alarm at the findings and is seeking clarification from the parties, as placing tracking cookies without a user's consent is strictly prohibited. In early 2023, the Dutch DPA had already warned all parties involved in the election campaign. Other political parties were also found to be loading information from sites like Twitter, LinkedIn, and YouTube, which could enable these sites to place cookies on users' devices. (November 2023)

Dutch employee insurance agency places illegal cookies

A Dutch employee insurance agency commissioned by the Ministry of Social Affairs and Employment illegally collected data from beneficiaries, tracking and analyzing visitors' behavior on their websites to investigate potential illegal stays abroad while receiving unemployment benefits. This excessive monitoring lacked legal basis and was discontinued in early 2023, as concluded by the government's standing law firm. Around 3,600 investigations were started by the insurance agency while the illegal cookies were in place. This led to the adjustment of "unemployment benefits" 460 times. Later research showed that the agency had known since 2020 that the cookies were not allowed. (August 2023)

The Dutch DPA will ensure that the insurance agency takes remedial measures, as they promised the Dutch DPA to rectify the situation. (November 2023)

What are the most relevant data protection updates?

Court rulings and claims

Summary proceedings against an advertising company

The Amsterdam Court has ruled that an advertising company cannot place tracking cookies on a man's system without consent as this is against GDPR. The company used these cookies to collect and analyze user data for commercial purposes, including targeted advertising. Despite the company's insistence that its partners are responsible for obtaining consent, the court found that the company itself cannot hide behind its partners when it comes to obtaining consent. The court ordered the company to stop placing tracking cookies on the man's systems immediately and give the man insight into his data within seven days. If the company does not comply, it will have to pay a penalty of €250 per day for each violation, with a maximum of €25,000. (October 2023)

Civil liability for Dutch university after data breach

In September 2021, the private data of many students a Dutch university were breached after a hack. For most students this concerned their contact information, however, for at least one student, medical information was breached as well, and that student held the university liable for its damages. The District Court ruled that the university had violated the GDPR, and the student was entitled to an individual compensation of €300. (October 2023)

Court: media company violated GDPR, but fine is unjustly imposed

The Dutch DPA imposed a fine on a media company due to violation of article 12(2) of the GDPR, as the media company standardly and in advance asked individuals exercising their right of access or erasure to confirm their identity with a copy of their identification document. The media company has appealed to the court, which ruled that there is a violation of article 12(2) of the GDPR as the company used a too rigid procedure to identify individuals, thereby creating an unnecessary obstacle. However, under the specific circumstances of the case, the court ruled that the Dutch DPA should not have imposed the fine. The fine of €525,000 does not have to be paid. (August 2023)

What are the most relevant data protection updates?

Court rulings and claims

Fine for credit registration bureau

On 30 July 2019, the Dutch DPA fined a credit registration bureau as the bureau would unjustly charge a fee to data subjects who exercised their right of access under the GDPR. The credit registration bureau objected to the fine with the Dutch DPA, however the Dutch DPA did not change its decision. The credit registration bureau then appealed to the court, which led to the decision that the Dutch DPA was allowed to impose a fine for not facilitating the right of access and charging a fee, however the fine was too high considering both aggravating and mitigating circumstances. The fine was reduced from €830,000 to €668,000. (July 2023)

"Consumentenbond" files class action against an internet search engine

The consumers' association and Stichting Privacy Belangen are pressing charges against an internet search engine company over extensive privacy violations. They demand that the company stops its constant surveillance and sharing of personal data through online ad auctions and pays consumers compensation of €750 for the damage. Since the announcement of this action on 23 May 2023, over 82,000 Dutch people have joined the mass claim.

Social media platform violates privacy of Dutch users

The Amsterdam Court has ruled that a social media platform violated the privacy of its Dutch users, according to a lawsuit filed by the consumers' association (Consumentenbond) and the Data Privacy Foundation (DPS). The judge decided that the platform failed to adequately inform its Dutch users about how it uses their data, thereby violating privacy laws. Facebook is found to have used data from Dutch users for advertising without valid consent, and external developers could access user data without sufficient informed consent from the users. Over 190.000 users joined the class action. The platform's parent company intends to appeal the decision. The consumers' association is considering to take further legal action or negotiate a settlement using this judgement. (March 2023)

What are the most relevant **AI updates**?

First Algorithmic Risks Report published

The Dutch DPA has issued its first Algorithmic Risks Report, which calls for additional measures to manage the risks of algorithms and artificial intelligence (AI). The report underlines that AI and algorithmic systems could potentially impact society and individuals in ways that violate basic rights. The DPA has cautioned that current regulations are inadequate to manage these risks and has urged the adoption of new legal safeguards. Additionally, the DPA has recommended that the government should take a more proactive role in mitigating these risks, including the supervision of the implementation and deployment of algorithmic systems. (July 2023)

Register of algorithms for the Dutch government

The Dutch government has established a register of algorithms in which the information about the algorithms used by public organizations should be published. With this register, the government is able to legally check algorithms for discrimination and arbitrariness. Citizens must be able to trust that algorithms comply with public values and (legal) standards and that there is an explanation of how they work. The Algorithm Register makes a significant contribution to making the application and outcome of algorithms transparent and explainable. This way, citizens, social organizations and media can critically follow and question the government and check whether it adheres to the rules. Publishing in the register is currently voluntary, however, the goal is to have a record of all government organizations with relevant algorithms in the register. (December 2022)

It has been proposed that registration of impactful algorithms will become legally mandatory and brought in line with the proposed EU AI Act. (July 2023)

Dutch DPA inquires about privacy at AI software company

The Dutch DPA has expressed concerns regarding organizations' handling of personal data when using Generative AI. The DPA has reached out to a software developing company for clarity on how it handles personal data during the training of their large language models. The software, based on an advanced language model trained with data, could potentially use sensitive and personal information. The DPA also has concerns about the accuracy of the information generated by the software and has joined other European privacy regulators in establishing a task force within the European Data Protection Board (EDPB) to coordinate activities. (June 2023)

DPA establishes first “Coordination Algorithms” board

The Dutch DPA has established the inaugural “Coordination Algorithms” board. This new department will be allocated an increasing budget starting from €1 million in 2023, steadily increasing until €3.6 million by 2026. The existing oversight on algorithms and artificial intelligence, which is spread among many different organizations, will remain intact. In addition to the new board, the DPA will reinforce its supervision on algorithms that unlawfully process personal data, for which the cabinet is allocating an annual budget of €2.61 million. The investment contributes to the ambition of the Dutch House of Representatives and government to prevent discrimination and arbitrariness and to promote transparency in algorithms that process personal data. (January 2023)

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

New focus of the Dutch DPA

The Dutch DPA published a document at the end of 2019 with its focus areas for 2020-2023, which were: data trade, digital government and artificial intelligence and algorithms. We expect that coming to the end of 2023, the Dutch DPA will publish new or extended focus areas for the coming years, 2024-2027.

We expect Generative AI to be one of the main focus areas, especially with the newly established inaugural "Coordination Algorithms" board and their allocated budget that will increase over the coming years, up to €3.6 million by 2026. The board will oversee the risks and effects of algorithms used in all sectors.

Increased budget of €3.8 million for Dutch DPA

The national budget for 2024 for the Dutch DPA has been increased by €3.8 million to €40.2 million. In reality, the budget increase mainly compensates wage and price increases, while the Dutch DPA's tasks are increasing in the field of AI and cybersecurity.

Increased budget for cookie and online tracking supervision by Dutch DPA

In the startup phase (2024-2026) the budget amounts to €500,000 per year. In addition to research and enforcement, the Dutch DPA intends to publish guidance and develop tools to facilitate investigations during this phase. From 2027 onwards, there will be a structural amount of €350,000 for investigations. The Dutch DPA will collaborate with the other supervisory authority on this subject, the Authority for Consumers and Markets, in accordance with their cooperation protocol.

Phasing out of third-party cookies in Google Chrome in 2024

Google announced that as part of the 'Privacy Sandbox' project, Chrome is phasing out support for third-party cookies. It will be a gradual phase out starting from Q1 2024, while new functionality cookies will be introduced that promise to preserve user privacy.

Norway

Contacts

Bjørn Ofstad

Partner, Deloitte Legal Norway

bofstad@deloitte.no

Hanne Pernille Gulbrandsen

Partner, Deloitte Legal Norway

hgulbrandsen@deloitte.no

Eirin Helen Hauvik

Partner, Deloitte Legal Norway

ehauvik@deloitte.no

What are the most relevant data protection updates?

Decisions of the Norwegian data protection authority (Datatilsynet)

January 2023 - Datatilsynet reprimanded the Church of Norway for unlawfully collecting information on members' newborns from the National Population Register for a month and a half after their authorization to receive this data had expired**.** The Church had permission to automatically receive birth notifications until October 2018, but continued to collect this data for an additional month and a half after the authorization had ended**.**

February 2023 – Datatilsynet imposed a fine of NOK 10 million (approximately €1,046,000) against a Nordic gym chain for various GDPR violations, including failure to provide sufficient information about the legal basis for processing personal data and refusal to comply with an erasure request**.**

March 2023 – Datatilsynet has fined Argon Medical Devices, a US-based company, NOK 2.5 million (approximately €260,000) for breaching the GDPR. The company failed to report a security breach affecting the personal data of its European employees, including those in Norway, within the 72-hour deadline required by the GDPR. The breach involved personal data that could be used for fraud and identity theft, and the company's delayed notification was considered an aggravating factor.

May 2023 – Datatilsynet banned the central Norwegian office for official government statistics Statistic Norway (SSB) from collecting live data from grocery story receipts combined due to insufficient legal basis according the GDPR Article 6(3). The data would be combined with bank account numbers and national identity numbers to produce statistics; however, the raw data would be stored for up to two years.

August 2023 – Datatilsynet issued an advance notification to suspend transfers of personal data by the Russian-owned taxi-app Yango to Russia due to concerns about a new Russian law granting a broad right of access to the data of taxi passengers. Datatilsynet will make a decision before the new Russian law comes into effect.

September 2023 – Datatilsynet plans to conduct several unannounced inspections of workplaces with young employees to ensure that they are not subject to illegal camera surveillance. Young workers are particularly vulnerable in the workplace, and the authority has received several tips about employers using cameras to monitor their employees. The goal is to raise awareness of the requirements for using camera surveillance in the workplace.

November 2023 - Datatilsynet issued an advance notification of an administrative fine and an order to bring the processing into compliance with the GDPR following an inspection at the Norwegian Labor and Welfare Administration (NAV) in September. Datatilsynet found a total of twelve violations of the GPDR, and in particular of the GDPR Articles 24 and 32. In its conclusion, Datatilsynet states that these violations are very serious and have been ongoing for a long time. Datatilsynet set the fine to NOK 20 million (approx. €1.7 million) which is high for a fine issued to a public sector organization.

November 2023 - Datatilsynet conducted inspections with over 100 Norwegian municipalities in 2023. Nineteen of these were visited by the authority as a follow up of the inspections. This has resulted in a report on the Datatilsynets findings as well as guidance to municipalities.

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

Decision against a social networking app

In September 2023, Grindr was fined approximately €6.5 million by Datatilsynet in 2022 for unlawfully sharing personal data with third parties for marketing purposes. Datatilsynet found that Grindr disclosed user data to third parties for behavioral advertisement without a legal basis and that consent collected for sharing personal data with advertising partners was not valid. In September 2023, The Norwegian Privacy Appeals Board upheld the fine, agreeing with Datatilsynet's findings. Grindr has appealed the Privacy Appeals Boards decision before a Norwegian court and the case is pending.

Meta and behavioral advertising

Datatilsynet imposed a temporary ban on behavioral advertising on Facebook and Instagram following the inaction by Meta after the decision by the Irish Data Protection Board in December 2022 and the subsequent decision by the Court of Justice of the European Union. Meta sought a temporary injunction against Datatilsynet's decision, but the Oslo District Court ruled in favor of Datatilsynet. Meta decided to appeal the decision but withdrew the appeal when the case was brought to the European Data Protection Board to make the temporary ban permanent and to extend it to the entire EU/EEA. This legal dispute is part of a broader trend where digital firms are offering "pay-or-consent" options, allowing users to pay for an ad-free experience or consent to targeted advertising. This development reflects the ongoing debate about privacy and targeted advertising on social media platforms.

Other news from Datatilsynet:

- Datatilsynet has published important guidance on the national regulation of electronic surveillance of employees, guidance on the EU-US data protection framework and guidance on the streaming of sport events for children.
- The Regulatory Sandbox has become permanent with a fifth round of applications opened. Datatilsynet has published reports in the following projects in 2023:
    - Simplifai and NVE
    - Ruter
    - Ahus
    - Doorkeeper

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

- Datatilsynet has met with over 100 public organizations and private businesses to map the needs and expectations concerning future guidance from the Datatilsynet. Datatilsynet asked specifically about challenges businesses are facing when working with the GDPR. Deloitte Legal was invited to participate. This may result in more guidance and a heightened focus on dialogue in 2024. Datatilsynet has yet to announce any strategic focus for 2024 and whether it will participate at the third coordinated enforcement action, which will concern the implementation of the right of access by controllers.
- Karianne Tung has become Norway's new Minister of Digitalization. She will oversee Norway's first cross-sectorial Ministry for Digitalization and Public Governance to be established on 1 January 2024. The new ministry will focus on accelerating digitalization, as well as the government's current initiative to improve and maintain trust in the public sector. In addition, the Norwegian government has announced a new national digitalization strategy for 2024.
- More data protection cases will likely end up in the court system in the year to come. Both Meta and Grindr have appealed decisions from Datatilsynet and the Privacy Appeals Board before the judicial system and the cases are pending in 2024.
- Datatilsynet and Norwegian Accreditation (the national accreditation body of Norway) have signed a collaboration agreement to accredit certification bodies under the data protection regulation in Norway. This marks the first step in creating a tool to ensure better compliance with data protection regulations in the country.
- The Tinius Trust has lodged a case against the Norwegian government challenging the laws concerning mass surveillance. The case revolves around the mass overwatching of Norwegian citizens by the Public Security Police (PST) and the E-tjenesten (an electronic service) The media is suing the state for mass overwatching, as the PST and E-tjenesten have the power to overwatch Norwegian residents. Several actors have raised concerns about the consequences of this overwatching for the media. Tinius' main argument is that the authorities should not be able to identify individuals who inform or communicate with journalists, as this would infringe on the freedom of the press and person rights, which are essential for the proper functioning of the press. The case is pending.

What are the most relevant **AI updates**?

AI Guidance from national authorities

- The Norwegian Equality and Anti-Discrimination Ombud has published guidance on how to prevent AI discrimination and ensure equality and anti-discrimination by design – inspired by the GDPR Article 25 (not available in English).
- The Norwegian Consumer Council published a report on the harms of Generative AI with a lot of focus on privacy from a consumer perspective. More guidance and opinions on harms and best practices related to AI is likely in 2024.

Romania

Contacts

Georgiana Singurel

Partner, Reff & Associates,
Deloitte Legal Romania

gsingurel@reff-associates.ro

Silvia Axinescu

Senior Manager, Reff & Associates,
Deloitte Legal Romania

maxinescu@reff-associates.ro

What are the most relevant data protection updates?

Guidance on usage of body cameras by public authorities (July 2023):

- The Romanian National Authority for the Protection of Consumers ("NAPC") carries out investigations with economic operators for the purpose of enforcing consumer law. Since May 2023, NAPC agents started wearing wear body cameras to capture images from inside the premises they are investigating.
- NAPC based the processing of personal data through the use of body cameras on its legal obligation, citing that the laws establishing the competencies of NAPC also empower the authority to conduct inspections at economic operator's premises.
- ANSPDCP conducted an investigation into the practices of the NAPC and concluded that the authority did not have a valid legal ground for the data processing, as the legal obligations cited by NAPC did not expressly mention the use of body cameras in the inspection activity.
- As a result, ANSPDCP re-affirmed its stance on the use of body cameras, stating that in its previous practice, it did not find any express legal obligations which mandated that public authorities (namely, police agents acting in the course of duty) use body cameras in exercising their inspection and control duties, therefore the processing took place without a valid legal ground, thus infringing the lawfulness principle.

Decision regarding the criteria for accreditation of bodies monitoring compliance with codes conduct (May 2023):

- ANSPDCP issued a decision approving the criteria for accreditation of bodies monitoring compliance with codes of conduct ("the Criteria"), pursuant to article 41 of the GDPR.
- The Criteria includes, among others, clarifications on the requirements of independence, conflicts of interest, expertise and governance.
- Up until this point, in Romania, no code of conduct has been developed or approved.

What are the most relevant data protection updates?

Individual (natural person) qualified as controller by the ANSPDCP

An individual was fined €450 following an investigation which concerned the disclosure of personal data on social media, in which the individual was qualified as the data controller. ANSPDCP found that the natural person processed personal data without observing the principle of lawfulness (article 5(a) of the GDPR), as they posted on social media names, surnames and city of residence of other natural persons without their consent, or reliance on another legal basis for the processing.

Disclosure of video footage on Facebook

A fine of €10,000 was imposed on a local gym for disclosing personal data (video containing images of several data subjects) on its Facebook page and failing to delete the video following a request by one of the data subjects. ANSPDCP found that the controller processed personal data (including sensitive data, as one data subject's racial origin was disclosed in the video caption) without a legal basis and that it had not adopted sufficient technical and organizational measures to ensure the confidentiality of the data captured through its CCTV system. On top of the fine, ANSPDCP also imposed corrective measures, such as ordering the controller to implement adequate policies and procedures aimed at ensuring lawful processing of personal data.

Cookies

In 2023 ANSPDCP maintained its focus on online activities, having sanctioned multiple economic operators for failing to observe the rules on cookies implementation. Among these cases, an electricity supplier was notably fined €40,000. During the investigation, ANSPDCP found that the company's website installed non-essential cookies without the data subject's consent and, moreover, that clicking on the 'Reject cookies' button did not have any effects on the already installed cookies which were installed and stored on the user's device for a period of time. The fine was applied in an investigation which started as a result of a data breach (for which a separate fine of €25,000 was applied).

Unsolicited commercial messages

In several investigations, the authority concluded that controllers sent commercial messages (via e-mail and/or SMS) either without having obtained the data subject's prior consent, or after the data subject had opposed to receiving such messages and without observing the data subject's opt-out. Fines applied ranged between €1,000-€3,000.

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

Fine of €110,000 applied to Rompetrol Downstream SRL (downstream gas operator)

This case concerns the unlawful disclosure of personal data of the company's clients, which were then used for fraud purposes. The controller had reported multiple data breaches between July 2021 and January 2022, following which ANSPDCP opened an investigation. The authority found that customer data from the company's own software had been repeatedly accessed by the staff and used in an unauthorized manner, having been disclosed for the purpose of obtaining loans in the data subject's name. As a result, ANSPDCP held that the controller was in breach of articles 32(1)(b), 32(2) and 32(4) of the GDPR and considered the fraudulent nature of the subsequent processing operations.

Fine of €70,000 applied to Uipath SRL (technology company)

The fine was imposed by ANSPDCP as lead supervisory authority, as the case concerned an international data processing. Uipath notified ANSPDCP of a data breach consisting of personal data of approximately 600.000 users of the Uipath Academy Platform (learning platform) which was unauthorizedly disclosed and accessed. To determine the fine amount, the ANSPDCP took into consideration, among others, the technical settings of the storage space which allowed unauthorized access to the personal data of the users of the Academy Platform, the fact that the incident consisted of the publication of personal data on a third-party website, information brought to the knowledge of the controller by a third-party, and the negligence of the controller.

Cumulative fines of €40,000 applied to Dante International S.A. (operator of e-commerce platform eMAG, with an online presence in Romania, Hungary and Bulgaria)

The Hungarian DPA informed ANSPDCP of potential breaches of the GDPR by Dante International S.A, following complaints from three Hungarian data subjects. ANSPDCP investigated the controller's practices as lead supervisory authority and cooperated with the Hungarian DPA, pursuant to article 60 of the GDPR, in order to reach a final decision in the case. The controller was fined for breaching articles 12(2), 17(1) and 6(1)(a) of the GDPR.

What are the most relevant **AI updates**?

The National Strategy for AI in 2023-2027

- In July 2023, the Authority for the Digitalization of Romania issued the National Strategy for AI ("the Strategy"), which establishes the public policy centered around the wide-scale adoption of AI.
- The Strategy enshrines the principle of data protection and data confidentiality as prerequisite for developing and adopting AI. However, the Strategy is a document focused on AI regulation and does not specifically address the intertwining between AI and data protection.

Order No. 20484/2023 regarding the establishment of the Romanian Committee for AI

- The Romanian Committee for AI (RCAI) is a public body organized within the Ministry of Research, Innovation and Digitalization, whose main attributes are regulating, coordinating, monitoring and evaluating activities revolving around AI.
- One of the attributes of the RCAI is to issue opinions on any relevant aspects regarding the development and deployment on AI.
- So far, the RCAI and ANSPDCP have not issued any news on their potential collaboration and/or cooperation in the field of AI, nor have any AI related decisions have been issued by any of the institutions.

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

Digitalization of the public administration

Romania allocated 6.5% of the funds received from the EU via the Recovery and Resilience Plan (NRRP) to the digitalization of public administration.

According to the targets stated in the NRRP, in 2024 we expect to see that at least 30 public institutons will be fully connected and integrated in the governmental cloud, thus changing the way citizens' personal data will be processed by public authorities.

To support the transition to the governmental cloud, the following targets have been achieved so far:

- In 2022, two pieces of legislation came into effect: Government Ordinance No. 89/2022 regarding the establishement, administration and development of the **governmental cloud platform** and Law No. 242/2022 regarding the **National Platform for Interoperability**.
- In 2023, the Minitstry of Research Innovation and Digitalization signed the contract for migrating the public administration data to the cloud.

Spain

Contacts

Rodrigo González

Partner, Deloitte Legal Spain

rgonzalezruiz@deloitte.es

Carlos de Jorge

Senior Associate, Deloitte Legal Spain

cdejorge@deloitte.es

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

Amendment to the Law 3/2018 on Data Protection and Guarantee of Digital Rights

- Relevant modifications have been introduced into the Spanish regulatory framework in the field of personal data protection, particularly in relation to the **administrative proceedings before the Spanish Data Protection Authority** (AEPD).
- The Spanish Data Protection Authority now has the possibility of carrying out **investigative actions through digital systems** (such as videoconferencing or other similar systems).
- In view of the nature of the facts and the circumstances of each specific case, the AEPD, after hearing the data controller or data processor, may **issue a warning**, as well as require them to adopt corrective measures aimed at putting an end to the possible breach of data protection legislation. This warning procedure shall have a maximum duration of **six months**.
- A new feature is introduced whereby, **once a complaint has been admitted** for processing, **if the data controller or data processor proves that it has adopted measures** to comply with the applicable regulations, the AEPD shall decide **to file the complaint**.
- On new developments regarding **time limits** for the sanctioning procedure:
  - The duration of the sanctioning procedure is modified from nine to 12 months;
  - The maximum duration of the investigation phase will be 18 months (as opposed to the 12 months previously established).;
  - The above-mentioned warning procedure will have a maximum duration of six months; and
  - Finally, it is determined that the AEPD may establish models for the submission of complaints, which will be of compulsory use for data subjects wishing to file a data protection complaint.
- Entry into force was 10 **May 2023**.

What are the most relevant data protection updates?

Law 2/2023 for the protection of whistleblowers and fight against corruption

- This law transposes **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 **aim of this law** is to provide adequate protection for whistleblowers against retaliation for reporting irregularities or certain breaches of the law. **Entry into force was 13 March 2023.**
- The **material scope of application** of the Whistleblowing Directive is limited to "acts or omissions that may constitute infringements of European Union law". This law extends the scope of application to criminal offences and serious or very serious administrative infringements, including those that cause economic loss to the Spanish Tax Authority and Social Security.
- The **subjective scope of application** includes: i) **entities**: companies with more than 50 employees, as well as, political parties, trade unions, business organizations, foundations and public administrations; and ii) **whistleblowers**: people who maintain professional or labor relationships with entities in both the public and private sectors (public employees, employed workers, self-employed workers, shareholders, administrators, directors), as well as those who have already ended their professional relationship, volunteers, interns, trainees or even job applicants.
- This law establishes that the administrative body of the company (board of directors, sole administrators, etc.) is considered as the data controller for the processing of the internal information system. However, the AEPD has clarified that **it is in fact the Company the data controller** when processing all the information in the context of the whistleblowing channel.
- **Entry into force was 13 March 2023.**

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

Circular 1/2023, of 26 June, on the application of article 66(1)(b) of Law 11/2022, of 28 June, General Telecommunications

- This circular deals with the right of users **not to receive unsolicited calls,** previously established in article 66(1)(b) of the General Telecommunications Law 11/2022.
- This article establishes the right not to receive unsolicited calls for commercial communication purposes, **unless the user has given prior consent** to receive this type of commercial communication, or the communication **can be supported by another legal basis** for the processing (Article 6(1) of the GDPR).
- From 29 June 2023, **users will be able to receive calls only if they have previously given their consent, or if the calling company can demonstrate that it has a legitimate interest** in making the call, outweighing the user's right not to receive it, and they have not exercised their right to object.
- The circular specifies that, in order for the company to justify its **legitimate interest**, the user **must have a previous relationship with the company**, having purchased its products or services, and the products offered by the company must be similar to those contracted previously. This option only applies to calls from the same company with which the relationship was established and not to other companies, even if they belong to the same group of companies.
- In addition, if the contractual relationship is no longer in force and the user **has not made any other request or interaction with the company in the last year, they will not be able to call**.
- **Entry into force was 29 June 2023.**

What are the most relevant data protection updates?

Code of Conduct - AUTOCONTROL's Code of Conduct for "Data processing in advertising activity"

- Autocontrol is the independent advertising self-regulatory organization (SRO) in Spain. On 27 January 2023, this organization approved a code of conduct applicable to all its members which includes a way to resolve data protection and advertising complaints from citizens more quickly.
- This is the first code of conduct approved by the AEPD in accordance with the provisions of articles 40 and 41 of the GDPR.
- This code applies to the processing of personal data for advertising purposes or that relate to advertising carried out by companies adhered to this code, such as the sending of commercial communications, promotional campaigns carried out for the purpose of collecting personal data, the use of cookies and equivalent technologies for behavioral advertising or profiling for advertising purposes, among others.
- The most important aspect of the code is the regulation of a system for the out-of-court settlement of disputes between the companies adhered to the code and the data subjects regarding the processing of their data in the field of advertising. From 1 January 2021, an online form will be available to individuals, who consider that the data protection legislation has been breached in an advertising activity, to lodge a complaint against these companies.
- In this sense, the AEPD will offer a mediation system (mandatory only for member companies) that will allow the parties to reach an agreement within 30 days and, if this is not achieved, the interested parties will be able to request a decision from Autocontrol's jury of advertising.

What are the most relevant data protection updates?

Guidelines issued by the Spanish Data Protection Authority (AEPD) - Amendment of the guidelines on the use of cookies

- The actions of accepting or rejecting cookies must be presented in a prominent place and format, and **both actions must be at the same level**, **without making it more complicated to reject them than to accept them**. The guide includes new examples of how these options should be displayed, offering guidance on, among other things, the color, size, and location in which they must appear.
- In the case of personalization cookies, if the user chooses them (for example, to choose the language of the website or the currency in which they wish to carry out transactions), these are **technical cookies** that do not require consent, and cannot be used for other purposes.
- However, if it is the publisher who makes this type of decision about personalization cookies, based on the information obtained from the user, they must inform the user of this fact and give them an opportunity to accept or refuse them. In this case, the publisher could not use them for other purposes either.
- The guide points out that there are certain cases in which non-acceptance may prevent access to or use of all or part of the service, as long as the user is informed, and an alternative (both free and subject to payment) is offered.

Report nº 0038/2023

- Various aspects relating to the **exercise of the functions of the Data Protection Officer ("DPO")** are analyzed:
  - **The controller may or may not take decisions based on the advice of the DPO,** since it is the controller who ultimately determines the ends and means and who assumes the possible consequences that the processing activities carried out may have on the rights and freedoms of individuals.
  - The DPO may have **access to any type of procedure or document necessary for the exercise of its functions** (as long as it is duly justified), **without the data controller being able to refuse on the grounds of the existence of a duty of confidentiality.**
  - **The functions listed in article 39(1) of the GDPR is not an exhaustive list.** The DPO may take on other additional tasks (for example, keeping records of processing activities). However, the assignment of other tasks must in any case not involve direct intervention in the decision-making process regarding the purposes and means of the processing.
  - **The DPO plays an important role as a liaison between the controller and the processor and the supervisory authority**. Our national rules provide for a mechanism for the transfer of complaints made to the DPO and that any complaints made to the AEPD must be followed by a report issued by the DPO.

What are the most relevant data protection updates?

Guidelines issued by the Spanish Data Protection Authority (AEPD) - Report nº 0098/2022

- The AEPD answers **if it is permissible** under data protection law "**the installation of biometric systems to control all access to entertainment stands**, making it possible to identify unambiguously the supporters who access these stands".
- In order for biometric data to be processed, one of the situations listed in article 9(2) of the GDPR must occur.
- In this sense, the AEPD indicates that **this biometric identification** cannot be carried out in a unique or obligatory manner on the basis of the "essential public interest" (article 9(2)(g) of the RGPD), since this should be provided for in a legal provision with the force of law and, nowadays, this **specific legislation does not exist in Spain**. The actual legislation only permits the implementation of **additional security measures (and not biometric identification)** for any competition or sporting event classified as high risk, or for venues that have been subject to closure sanctions such as the promotion of systems for verifying the identity of persons seeking access to sporting events.
- On the other hand, the use of biometric recognition systems is allowed to control access to football stadiums, based on the explicit, informed and voluntary consent of the fans (article 9(2)(a) of the RGPD), as Veridas/dasGate has done with its C.A. Osasuna and Málaga C.F. facilities.

Guide to help companies and public authorities to comply with data protection when creating data spaces

- The guide has been drafted due to the exponential growth that technology is experiencing and, consequently, the need to use personal data for very diverse purposes, including the creation of large-scale data spaces at both national and European level.
- The guide fosters the idea of **data protection by design** in the creation of data spaces, focusing on **anonymization** as a security measure.
- Data protection officers play a key role in the management of these spaces, as they must assess the risks that their creation poses to the rights and freedoms of data subjects. Ethics must also be a fundamental principle to be taken into account in the development of data spaces.

The AEPD launches the ValidaCripto tool for the evaluation of cryptographic systems.

- Its objective is to provide an effective solution for **verifying the suitability of the cryptographic systems used in the processing of personal data**, selecting the most suitable from the list of controls proposed. The data can be stored and loaded in a local file, under the full control of the user, and allows reports to be generated.
- The use of cryptographic systems allows sensitive information to be encrypted, transforming it into a seemingly unintelligible set of data, which helps to mitigate the risks of a possible breach of personal data.

What are the most relevant data protection updates?

Guidelines issued by the Spanish Data Protection Authority (AEPD) - Guidelines on the processing of employees' biometric personal data in the employment (monitoring) context

- The AEPD has recently issued specific guidelines in order to establish the criteria to be followed for the processing of biometric personal data concerning employees to purposes related with the monitoring and register the working hours.
- These guidelines determine that the exception established in article 9(2)(b) of the GDPR is not applicable. We have to remind that this exception sets forth that the biometric personal data shall be permitted when "*processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or member state law or a collective agreement pursuant to member state law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.*"
- However, since the Spanish applicable labor regulation does not allow the use of biometric personal data to monitor and register the employees' working hours, this exception cannot be applied.
- On the other hand, the AEPD considers that the exception established in article 9(2)(a) of the GPDR (explicit consent) could be applicable provided that the data controller implements an alternative way to achieve the same purpose that not implies the processing of biometric personal data. Nevertheless, in such event in which an alternative way to achieve such purpose can be implemented, the processing of biometric personal data is no longer necessary. Therefore, this processing of biometric personal data will not be approved when the data controller conducts the required data protection impact assessment, regarding that the processing cannot be considered necessary in order to reach the intended purposes.

What are the most relevant data protection updates?

Sanctions imposed by the AEPD - PS/00375/2022 (23 October 2023)

- The complainant informed BBVA that her telephone number, credit cards, among others, had been stolen and asked the immediate cancellation of all the products she had contracted with the bank.
- Even though BBVA blocked the credit cards, that did not prevent the subscription and use of financial products by the impersonator, including unauthorized charges, transfers and transactions. In addition, BBVA demanded payment of the debt to the complainant, and they registered her in a debtor's list.
- The Spanish Data Protection Agency (AEPD) fined BBVA with €1.2 million for violating:
    - **Article 6(1) of the GDPR:** BBVA failed to apply a legal basis for processing when subscribing products with impersonators and transferring complainant's personal data to debtor's list.
    - **Article 25 of the GDPR:** BBVA failed to apply the principle of privacy by design by not implementing privacy measures in its fraud management process in the event of identity theft. Identity theft may pose a certain risk to the financial institution and BBVA must therefore take measures to mitigate this risk.

      BBVA's risk analysis approach was business/organizational/technological; They were based on avoiding fraudulent practices that result in harm to the entity and indirectly harm the client. They did not have a risk analysis focused on how it could affect the rights and freedoms
      of clients.
    - **Article 32 of the GDPR:** The bank must be proactive and have measures in place to ensure data security when a client reports the theft of personal items (e.g., blocking online accounts, changing passwords, internal communication and coordination within the organization, etc.). In addition, the bank must prevent further financial or personal damage.

      The theft of IDs and bank cards is not a mistake, but a risk that must be anticipated and mitigated by the controller. Since the theft was reported, the bank did not supervise the incident and were able to contract several products, which shows that this is not a specific event and that BBVA is violating the right to data protection.
- The position of the AEPD is oriented towards the adoption of additional due diligence measures by entities in the financial sector, such as:
    - Review of internal procedures and standards, in order to identify whether they are adapted to privacy principles by design and by default; and
    - Review of fraud prevention processes and policies, with the aim of identifying and verifying measures aimed at avoiding the risk of identity theft in the physical or online environment.

What are the most relevant data protection updates?

Sanctions imposed by the AEPD - PS/00331/2022 (31 July 2023)

- The AEPD fined with €2.5 million a financial entity (OpenBank) for the following infringements: (i) €1.5 million for non-compliance with article 25 of the GDPR (privacy by design) and €1 million for non-compliance with article 32 of the GDPR (security measures).
- In general terms, the AEPD criticizes the bank's lack of procedures and secure means to receive certain PML documents from its clients, taking into account their sensitivity. The request and the collection of these documents were carried out by e-mail, which the AEPD did not consider sufficiently secure. In fact, and more specifically, it should be highlighted the fact that a more secure system was not used to load the data, such as the "customer portal" on its website.
- In addition, the AEPD considers that "financial data" should not be considered as "high-level" data in the strict sense and in all cases, but that the adoption of technical and organizational measures must be proportionate to the impact that could result from a loss of control or unauthorized access of this type of data.
- It is necessary to distinguish between data relating to the economic situation (medium risk), the financial situation (medium risk) and data relating to means of payment (high risk), arguing that it is not only important the nature or category of the data concerned but also the implications and risks associated with their processing.

Sanctions imposed by the AEPD - PS/00553/2021 (9 May 2023)

- The AEPD fined the organizers of the Mobile World Congress with €200,000 for not carrying out a proper data protection impact assessment (DPIA) on the use of facial recognition systems to control access to the Mobile World Congress 2021, which involved the processing of biometric data.
- The impact assessment submitted by the defendant was "merely nominal", since it did not examine the substantive aspects of the system, nor did it assess the risks, the proportionality and the necessity of its introduction, nor its impact on the rights and freedoms of the persons concerned.

Sanctions imposed by the AEPD - PS/00636/2022 (18 July 2023)

- The AEPD sanctioned a telecommunications company (DIGI SPAIN TELECOM) with €70,000 because said company provided to an unauthorized third-party with a duplicate SIM card of the legitimate owner (sim-swapping). The AEPD stated that there was an infraction due to violation of article 6 of the GDPR, which refers to the legal basis for processing.

What are the most relevant data protection updates?

Sanctions imposed by the AEPD - PS/00413/2021 (20 March 2023)

- The Spanish Data Protection Agency (AEPD) sanctioned a telecommunications company (ORANGE) with €100,000 for requesting the ID to a customer and make a copy of such document in order to verify his identity and, therefore, deliver a package to this customer.
- The AEPD determines that there are indications of a violation of article 5 of the RGPD, specifically the principle of data minimization. In this regard, the AEPD states that there are other product delivery procedures by which the identity of the recipient can be verified without needing a photograph of the ID.
- Furthermore, it points out that the ID contains numerous personal data that are neither adequate nor relevant for the accreditation of the person. In general terms, the AEPD emphasizes that the moment of conclusion of the contract, where the identification document is requested to prove the identity of the person with whom it is contracted, has nothing to do with the moment of delivery of the product.
- In addition, requesting the ID image at the time of delivery of a product contracted at a distance is not only not considered legal but is also considered inappropriate, not relevant and not limited.

Sanctions imposed by the AEPD - PS/0012/2022 (18 July 2023)

- A fine of €20,000 is imposed on a real estate company due to the disclosure of a former employee's private information (including his Spanish ID) to third parties by email (breach of article 5(1)(f) of the GDPR).
- The AEPD states that since the Spanish ID uniquely identifies a natural person, this personal data must be considered as particularly sensitive. The reason is that a third-party will be able to impersonate the identity of any natural person with absolute ease with the risks that this entails for the privacy or assets of the impersonated person. This risk of usurpation or identity theft in the use of the Spanish ID also entails risks of fraud or financial loss, which reinforces the consideration of this data as sensitive.

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

Preliminary investigations against a Generative AI platform

The AEPD has opened an ex officio preliminary investigation against the American company OpenAI, owner of the ChatGPT service, for possible non-compliance with data protection regulations. The AEPD asked the European Data Protection Board to include the ChatGPT service as a topic for discussion at its plenary meeting, considering that there are global data processing activities that may have a significant impact on people's rights, and this may require harmonized and coordinated action at the European level in application of the GDPR. The committee decided to set up a task force to promote cooperation and exchange of information on actions taken by data protection authorities.

What are the most relevant **AI updates**?

Publication of the Royal Decree nº 817/2023, that established a controlled environment in order to test the compliance with the Proposal for a Regulation on Artificial Intelligence and in order to establish harmonized rules on the use of artificial intelligence (sandbox)

- The Spanish government has published a Royal Decree with the objective of creating and designing a controlled environment to allow public and private organizations to perform tests about the compliance with the Proposal of a Regulation on Artificial Intelligence.
- This environment implemented by the Spanish government will permit to test products, software and other tools (such as Generative AI) based on artificial intelligence in order to assess whether such tools have been designed in accordance with the referred European regulation and the applicable local regulations.
- In particular, this sandbox will permit the public and private organizations that desire to test their AI tools to evaluate whether such tools put citizens' fundamental rights in risk and how to configure or modify the design of their tools in order to guarantee such rights and in order to comply with applicable European and local regulations.

Sweden

Contacts

Lisa Bastholm

Senior Manager, Deloitte Legal Sweden

lbastholm@deloitte.se

Michelle Smed

Consultant, Deloitte Legal Sweden

msmed@deloitte.se

What are the most relevant data protection updates?

Four companies must stop using Google Analytics

The Swedish Supervisory Authority, Integritetsskyddsmyndigheten ("**IMY**") finished its investigations in July 2023 regarding four companies' use of Google Analytics following a complaint from the organization NOYB. In its investigation, IMY found GDPR violations regarding data transfer requirements.

For the transfer of personal data to the US all of the companies had used the standard contractual clauses ("SCC"). In the decision from IMY, it was concluded that there were not sufficient safety measures in place to uphold an essential level of protection for the transferred personal data and that the data transfer was violating the GDPR.

IMY also touched upon the question of statistics data. In the decision, it was stated that statistics data in Google Analysis is considered personal data, since they can be used to identify a person (together with the other data Google holds).

Eventually, one of the companies was fined SEK 30,000, and another SEK 1.1 million. The other two companies did not receive fines since they had implemented some safety measures. One of the companies quit using Google Analytics themselves, and the others were ordered to cease the use of Google Analytics.

Administrative fee against Swedish tech company

The Swedish Supervisory Authority, Integritetsskyddsmyndigheten ("**IMY**") issued an administrative fine against a Swedish tech company of SEK 58 million (approx. €5 million) for a lack of transparency towards data subjects. The main reasons for the fine was lack of sufficient information to the data subjects on how their personal data was processed by the company. Further, IMY stated that the information of the data processing should have been more specific, and that it must be easy for a data subject to understand how its personal data is used.

The case also concerned the data subjects' right to request and access. When a data subject requested access, the company had divided their personal data into "layers", based on what the company considered to be most relevant. For example, one layer consisted of customer data (contact details, payment details) whilst another layer consisted of technical data. IMY did not find this was a concern. On the contrary, dividing personal data into layers can make it easier for the data subject to understand the information,

One notable finding by IMY is that, when the data subject is exercising its right to access, information given by the controller that could be technical or otherwise hard to understand may need to be explained in the data subject's native language. In light of IMY's findings, organizations may have reason to review the language in which information is provided to data subjects.

What are the most relevant data protection updates?

Swedish publishing company – Administrative fine of SEK 13,000,000

The Swedish Supervisory Authority, Integritetsskyddsmyndigheten ("IMY") investigated and issued a fine to a publishing company for profiling of its website visitor without consent. The company had collected personal data from various sources and used it to for direct marketing on its website, by e-mail and phone. The personal data included browsing history for purchases from other group companies, combined with personal data (e.g., gender, postal address, car ownership) purchased from third parties. The company has used "legitimate interest" for the marketing as legal basis, arguing their interest of marketing outweighed the data subjects.

In its decision, IMY argued that data subjects can not expect that their behavior data is collected just because they visit a certain website. Nor can they expect their behavioral data to be combined with data from other registers for the purpose of contacting them for telemarketing or direct marketing. Further, IMY stated that this type of extensive profiling cannot rely on the legal basis "legitimate interest", but the data subject's consent must be collected.

On the contrary, IMY further stated that it would have been possible to use the legal basis "legitimate interest" for marketing by e-mail or phone not based on browsing history. In conclusion, the company was considered having violated article 6(1)(f) of the GDPR, as the SA argued that the legitimate interest of the data subjects outweighed the companies in this case.

Insurance company – Administrative fine of SEK 35 million

The Swedish Supervisory Authority, Integritetsskyddsmyndigheten ("IMY") has fined an insurance company SEK 35 million after finding flaws on their webpage, making it possible to access customer data of 650,000 customers during the period October 2018 to February 2021. IMY was alerted of the breach when a person reported the access to other policyholders' documents without any kind of login, by simply replacing a few numbers in the web link. The concerned data was highly sensitive in nature as it disclosed detailed health information, financial information, social security number, insurance holdings and contact details.

In its decision, IMY stated that the processing managed by an insurance company mandates high standards with regards to security measures, such as authorization control, encryption, logging, access control and mitigation of technical vulnerabilities. Taking into account the long period of time it was possible to access other accounts, IMY's opinion was that the company should have noticed this and that a severe breach of the principle of confidentiality (article 5(1)(f) of the GDPR) had occurred.

What are the most relevant upcoming data protection developments?

IMYRS 2023:1 – Guidance for data protection in practice

In June 2023, IMY published a guidance based on a survey of data protection officers in over 800 organizations. The aim with the report is to provide an indication of the conditions under which data protection is applied in organizations required to have data protection officers. The report summarizes the key observations from the survey, and what the main gaps in GDPR compliance for DPO's are. Some key findings are lacking time allocation for the DPO's tasks, and insufficient training in data protection. A quarter of the DPO's lack specific time allocation, and half of the DPO's participating feel that the allocated time is not long enough. Furthermore, the report highlights that only four out of 10 organizations works continually and systematic with data protection issues. IMY has identified that one of the biggest challenges is to create practical procedures and coordinate the data protection rules with an organization.

IMYRS 2023:2 – Reported data breaches 2022

In August 2023, IMY published a summary report of reported data beaches during 2022. The summary shows that 70% of the reported data breaches come from the public sector. It is also shown which breaches that are most common: 63% of all reported breaches derived from unauthorized disclosure, such as wrongly sent e-mails or incorrect management of personal data.

The report also includes a comparison with the other Nordic companies of reported data breaches between 2019-2022. IMY's report shows that Denmark is the country with the highest number of reported personal data breaches, followed by Sweden and Finland. In relation to its population, the report shows that Sweden has fewer notifications than both Denmark and Finland. To avoid an minimize the risk data breaches, IMY has included preventive guidelines which, amongst other things, include recommendations on a systematic information security work, active authorization management and to have a good security environment and culture.

IMYRS 2022:3 – Guidance on camera surveillance

In November 2023, IMY published a guideline on camera surveillance. In the guidelines, basic GDPR principles and how to comply with those when conducting camera surveillance are explained. This includes for example, the importance of the basic general principles in article 5 of the GDPR, how to determine which legal basis is applicable and when a DPIA must be conducted. The guidelines also highlight the importance of information (regarding the camera surveillance) to data subjects, and requirements to do so by setting up signs in connection with the cameras or the area under surveillance.

The guideline also include a more in-depth description on how to use the legal basis "legitimate interest" for camera surveillance purposes, with practical suggestions on which interests that can be relevant. Retention period for camera surveillance is also touched upon, and how to determine that personal data captured are only stored for as long as necessary for the purpose of the data processing.

What are the most relevant upcoming data protection developments?

IMYs investigation of identification requirements when requesting access to personal data

IMY has received several complaints from individuals regarding how a company processes their personal data. The complaints come mainly from people who have complained to a data protection authority in Germany and are mainly about individuals who have approached the company and requested the deletion of their personal data or access to the personal data that the company holds about them. In that process, the complainants consider that the company has imposed unreasonable requirements on them to confirm their identity. IMY has now initiated an investigation of the company.

IMYs investigation of online checkout process

IMY has received several complaints concerning a company's checkout service and has initiated an investigation of the company. The complaints mainly concern how the company retrieves and fills in personal data (on the website, in the check-out view) after the buyer has only filled in some personal data. Some of the complaints come from Swedish users, while others come from users in Germany and Finland but is investigated by IMY since the company is Swedish.

IMYs investigation of patient data in Outlook

IMY has initiated an investigation to find out whether a public authority is handling patient data correctly. The public authority has sent and stored personal data including health information in the e-mail system Outlook for a very long time. As health data, and more specifically patient data, requires a particular level of protection the authority might not be permitted to use the system for processing such personal data. Personal data about patients is particularly worthy of protection and therefore requires that it be handled in technical systems with high security. The investigation will focus on technical and organizational security measures used by the public authority to protect patients' personal data when using the e-mail system.

What are the most relevant **AI updates**?

Regulatory pilot project on AI

In March 2023, IMY reported on its first regulatory polit project regarding AI. Since the end of 2022, IMY has worked with Region Halland, Sahlgrenska University Hospital and the organization AI Sweden on a pilot project with regulatory testing activities for healthcare. The project focused on de-centralized AI, which could be used to determine the likelihood of backlashes for patients with certain conditions. IMY's role in the project was to advice on the compliance with data protection rules. IMY has now initiated the third round of their regulatory testing activities and are looking for a new project to engage it. Starting from 2024, testing projects will be a part of the supervisory authority's permanent missions.

Switzerland

Contacts

Paul de Blasi

Partner, Deloitte Legal Switzerland

pdeblasi@deloitte.ch

Audrey Soutter

Senior Manager, Deloitte Legal Switzerland

asoutter@deloitte.ch

What are the most relevant data protection updates?

New Federal Act on Data Protection ("nFADP")

Switzerland has implemented a completely revised federal law on data protection. The purpose of this revision was to adapt the Federal Act on Data Protection (from 1992) to today's social and technological conditions and to align it with European law (in particular the GDPR). Swiss companies must comply with this revised law since 1 September 2023. The nFADP applies to any data processing activities that have an effect in Switzerland, even if they were initiated abroad.

Main changes

The nFADP is "a GDPR-like" legislation and provides for certain (new) obligations which were not contained in the previous FADP, we would highlight the following:

- Only data relating to natural persons are covered by the nFADP;
- Genetic and biometric data now fall under the definition of sensitive data;
- Entities (data controllers or data processors) must keep a Register of Processing Activities (ROPA - comparable to the one required under the GDPR);
- Data subjects must be informed of any data processing (general notification obligation) and/or data transfer. In case of a data transfer, the notification shall include the country/ies concerned (e.g, "outside EEA" would not be sufficient) and the safeguards taken when necessary;
- A data processor may only transfer personal data to a third-party (subprocessor) with the data controller's prior consent (comparable provision under the GDPR);
- Under certain conditions, the data controller may have an obligation to carry out data protection impact assessments (DPIA - comparable provisions under the GDPR);
- Foreign data controllers must, under certain circumstances, designate a representative in Switzerland, notably if they process personal data of data subjects in Switzerland (comparable to the GDPR Representative);
- The data controller must report data security breaches to the Federal Data Protection and Information ("FDPIC") under certain circumstances; and
- The data controller may, but is not obliged, to appoint a data protection advisor as a contact point for the data subject and the FDPIC.

Implementation effort

Companies which are already compliant with the GDPR should have minimal changes to make to their documents and privacy processes. They should at least review their privacy statements and privacy policies and, if needed, adapt them to fulfil the nFADP requirements. For those that are not yet compliant with either the GDPR, or with the FADP, the entire nFADP implementation program will need to be implemented. In addition, it is worth reminding that Swiss companies shall comply with the GDPR, and take the necessary measures, if they:

- Process personal data of individuals located in the EU; and
- Offer goods or service to EU individuals or monitor the behavior of EU individuals.

What are the most relevant data protection updates?

Sanctions

Under the nFADP, responsible individuals are, on complaint, personally liable to a fine of up to CHF 250,000. When the violation is committed within a company, the responsible individuals of the penal provisions are in principle the individual managers or officers of the company. However, a company itself could be directly liable to a fine if the violation is of a minor importance (i.e., for fines up to a maximum of CHF 50,000) and if the identification of the responsible individual within the company requires disproportionate investigative efforts. Violations of certain new obligations and duties, such as keeping a register of processing activities or obligation to perform a data protection impact assessment are not liable to a fine.

Switzerland and the use of standard contractual clauses ("SCCs")

SCCs are one of the instruments a data exporter can use to contractually secure a data transfer to a country that does not have an adequate level of data protection. The FDPIC has recognized the EU standard contractual clauses, including all modules, subject to some modifications when necessary. More particularly, provisions related to the competent supervisory authority, applicable law and place of jurisdictions shall be adapted for the SCCs to comply with Swiss law and ensure an adequate level of protection.

Guidelines from the FDPIC

Guidelines for the realization of data protection impact assessment ("DPIA")

The FPDIC has published in August 2023 a document containing guidelines to be considered by data controllers when performing a DPIA. The guide provides information on how to implement the DPIA and the elements it must contain.

Guidelines for checking the admissibility of data transfer to a third country

The guideline published by the FDPIC intends to make it easier for data controller to check the permissibility of personal data transfer abroad. Based on a diagram, this guidance illustrates the case of a data transfer abroad in a country where the applicable legislation does not ensure an adequate level of protection and provides some solutions to implement such as including standard data protection clauses or binding corporate rules.

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

Swiss federal and public administrations and the use of cloud services

Use of the cloud infrastructure by federal and public administrations is currently a central subject in Switzerland. The Supreme Federal Court has already rendered four decisions in the same case regarding the use by the federal administration of cloud services offered by foreign cloud service providers. The question is whether the use of the cloud can be assimilated to an ordinary situation of subcontracting, for which it would be sufficient to conclude a contract with all the required guarantees (article 9 of the nFADP) or whether the use of the cloud by a public administration requires the adoption of specific legal provisions and, if necessary, prior validation by the Swiss legislator.

None of the four decisions have yet resolved this issue. A new decision from the Supreme Federal Court to settle this question is expected shortly.

What are the most relevant AI updates?

Federal Council examining regulatory approaches to AI

In a press released dated 22 November 2023, the Federal Council instructed the Federal Department of the Environment, Transport, Energy and Communications ("DETEC") to prepare an overview of possible regulatory approaches to AI by the end of 2024, and to involve all federal agencies responsible in the legal areas affected.

Key points

The Federal Council mentioned that the overview will notably focus on the following elements:

- **Compatibility with the EU AI Act and the Council of Europe's AI Convention:** The analysis will build on existing Swiss law and identify possible regulatory approaches for Switzerland that are compatible with the EU AI Act and the Council of Europe's AI Convention.
- **Compatibility with fundamental rights:** The analysis will examine the regulatory requirements with a particular focus on compliance with fundamental rights.
- **Technical standards, financial and institutional implications:** The implications of the different regulatory approaches will be taken into account in the overview.
- **Interdisciplinary cooperation:** The analysis will involve careful legal, economic and European policy clarifications and require interdisciplinary cooperation across all departments.

Timeline

This analysis should create the basis to issue a concrete mandate for an AI regulatory proposal in 2025.

United Kingdom

Contacts

Cavan Fabris

Partner, Deloitte Legal UK

cfabris@deloitte.co.uk

Katherine Eyres

Director, Deloitte Legal UK

keyres@deloitte.co.uk

What are the most relevant data protection updates?

Post-Brexit

As of 31 December 2020, the EU GDPR ceased to apply in the UK. The UK legislated its own version, known as the UK GDPR, which currently has few material differences to the EU GDPR. However, reforms are being introduced which will change this (see 'Data Protection and Digital Information Bill' below). The EU Commission adopted an adequacy decision allowing data to continue flowing freely from the EEA to the UK. This decision is due be reviewed by the Commission in 2024, and if not extended, the UK's adequacy status will expire in June 2025. Separately, the UK adopted an adequacy regulation allowing data to continue flowing freely from the UK to the EEA.

International data transfers

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 (EU SCCs) 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. There is a standalone international data transfer agreement (IDTA) and an addendum of the new EU SCCs covering transfers of UK personal data. For organizations exporting personal data from both the UK and EU, a combination of new EU SCCs and the UK Addendum has been frequently used to simplify transfer documentation.

The Data Protection (Adequacy) (United States of America) Regulations 2023 came into effect on 12 October 2023. From this date, UK organizations will be able to transfer personal data to US entities certified under the UK Extension to the EU-US Data Privacy Framework agreed between the US and the EU, without the need to implement further transfer safeguards.

The Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023

The Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023 ("**Regulations**") are due to come into force on 31 December 2023. The Regulations have the effect of providing that references to "fundamental rights and freedoms" pertain to the European Convention on Human Rights (which has been enshrined by the Human Rights Act 1998) instead of the Charter of Fundamental Rights of the European Union.

The right to a private life and right to freedom of expression will continue to apply in the new definition of "fundamental rights and freedoms". The right to the protection of personal data will not be carried across, but the right to a private life and protections in the UK GDPR and DPA 2018 will apply and have a similar effect in practice. These changes are unlikely to increase the regulatory burden on organizations.

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

UK Information Commissioner's Office (ICO) highlights

The ICO published various regulatory guidance and reports on a range of topics, including:

- AI Guidance (March 2023 update) – in parallel with the UK government's white paper on AI
- Technological Horizons Report (December 2023)
- Guidance on Employee Monitoring (October 2023)
- Data protection and journalism code of practice (July 2023) - submitted to Secretary of State.
- The ICO and the European Data Protection Supervisor (EDPS) have also signed a Memorandum of Understanding (MoU) regarding their commitment to cooperate internationally to uphold individuals' data protection and privacy rights.

What are the most relevant **AI updates**?

AI regulation

The UK government released for public consultation a white paper ("**AI regulatory whitepaper**") detailing plans for implementing a pro-innovation approach to AI regulation and a related impact assessment. The consultation closed on 21 June 2023.

Data privacy is obviously a key concern that arises in the context of the development and use of AI-powered technology. For the time being, these risks will need to be addressed through the existing data protection regime.

National Cyber Security Centre (NCSC) and US Cybersecurity and Infrastructure Security Agency (CISA)'s new "*Guidelines for Secure AI System Development"*

On 27 November 2023, the NCSC and CISA released guidelines for a secure AI system. These global guidelines are aimed at providers of any systems that use AI, whether those systems have been created from scratch or built on top of tools and services provided by others.

The guidelines are intended to assist stakeholders with making informed decisions about the design, development, deployment and operation of their AI systems.

Artificial Intelligence (Regulation) Private Members' Bill (PMB)

The PMB was introduced to the House of Lords on 23 November 2023. The main purpose of the PMB is to establish a central AI Authority to oversee the regulatory approach to AI.

If the PMB is enacted, the AI Authority would have wide-reaching powers to:

- Carry out various coordination and monitoring functions, including ensuring that relevant regulators take account of AI and conducting an AI gap analysis of current legislation and regulatory responsibilities and promoting interoperability with international regulatory frameworks;
- Assess and monitor risks across the economy arising from AI, conduct horizon-scanning, including by consulting the AI industry, to inform a coherent response to emerging AI technology trends;
- Support sandbox initiatives to help AI innovators get new technologies to market; and
- Accrediting AI auditors.

In carrying out its regulatory functions, the AI Authority will need to be guided by certain principles designed to strike a balance between responsible AI use and broader economic interests such as UK international competitiveness.

There is an extensive legislative process that the PMB would need to go through before it becomes law.

What are the most relevant upcoming data protection developments?

Data Protection and Digital Information Bill

The Data Protection and Digital Information Bill is currently working its way through the relevant UK parliamentary processes and, as at November 2023, will now proceed to the House of Lords for consideration. It will introduce various 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. This means increased divergence between the EU GDPR and the UK GDPR in some areas. Key changes include:

- Amendments in relation to use of personal data for scientific research purposes;
- New powers to require data from third parties, particularly banks and financial organizations, to help the UK government reduce benefit fraud;
- A proposed 'data preservation process' requiring social media companies to keep any relevant personal data which could then be used in subsequent investigations or inquests involving children who have died through suicide;
- Use of biometric data, such as fingerprints, to strengthen national security;
- Provisions aimed at digital verification services and customer data and business data; and
- Some updates to the process for data subject requests.

Some of the more detailed proposals relate to the following:

Cookies: Proposed reforms will remove the requirement to obtain consent to set certain types of analytics cookies and similar technologies. 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.

International data transfers: Proposed reforms will change the standard of protection from *essentially equivalent,* which is the standard referred to in the EDPB guidance for transfers of personal data from the EU to a third country, to a level of protection that might not be *materially lower* than the standard in the UK. It remains to be seen if there will be any material practical difference between these two standards.

Accountability framework: Proposed reforms will remove the following requirements: i) designation of a data protection officer under articles 37 to 39 of UK GDPR; ii) data protection impact assessments under article 35 of UK GDPR; and iii) maintenance of record of processing activities under article 30 of UK GDPR. Instead, organizations would need to maintain a "Privacy Management Programme", including appointing a suitable senior person 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. These reforms are most likely to benefit SMEs.

Overview of data protection and privacy services

Overview of data protection and privacy services

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

Some of the ***cross-jurisdictional data protection services*** are:

- Drafting or reviewing privacy documents and assisting in the implementation of data governance;
- Drafting privacy notices and cookie policies and banners for sites/ecommerce;
- Drafting and negotiating privacy/security clauses, data processing agreements, data transfer agreements, joint controllership agreements and other contracts;
- Carrying out risk assessments, data protection impact assessments, legitimate interests assessments and other privacy assessments, also in relation to the use of new technologies;
- Advising on data transfers related matters, carrying out transfer impact assessments, drafting standard contractual clause, binding corporate rules and global data transfer agreements, supporting in the identification of adequate supplementary measures;
- Supporting in the management of data breaches and of subject access requests and other privacy rights;
- Delivering trainings to employees and managers;
- Defining audit plans and carrying out the connected activities;
- Supporting in multi-jurisdictional projects and in extraordinary deals;
- Supporting in any procedure before the competent supervisory authorities;
- Assisting in any claim or litigation concerning personal data; and
- Providing DPO service or supporting the internal DPO.

In addition, some of the ***cross-jurisdictional AI-related services*** that are offered by Deloitte Legal privacy and data protection teams are:

- Conducting AI assessments, evaluating risks to data and people;
- Supporting in the identification of appropriate measures to avoid bias and discrimination, ensure fairness and correct errors and inaccuracies;
- Drafting clauses and contracts to stipulate relationships with users, suppliers, partners, allocating responsibilities;
- Carrying out audits on providers;
- Drafting transparency documents;
- Drafting appointments, policies and procedures, records in connection with the use of AI systems;
- Conducting trainings to create awareness in relation to the correct and safe use of AI systems; and
- Managing security incidents, litigations and relations with regulatory authorities.

Deloitte.
Legal