

# Cross-jurisdictional data protection, cybersecurity and AI overview

Recent updates and upcoming developments

December 2024 – Third Edition

# Index

3 [Introducing Deloitte Legal](#)

4 [Overview](#)

6 [National updates and developments](#)

7	<a href="#">Albania</a>	131	<a href="#">Greece</a>	244	<a href="#">Portugal</a>
15	<a href="#">Argentina</a>	138	<a href="#">Guatemala</a>	250	<a href="#">Romania</a>
21	<a href="#">Australia</a>	140	<a href="#">Hungary</a>	256	<a href="#">Senegal</a>
28	<a href="#">Austria</a>	146	<a href="#">Iceland</a>	262	<a href="#">Serbia</a>
31	<a href="#">Belgium</a>	151	<a href="#">Indonesia</a>	267	<a href="#">Singapore</a>
43	<a href="#">Bulgaria</a>	156	<a href="#">Italy</a>	277	<a href="#">Slovenia</a>
50	<a href="#">Cameroon</a>	166	<a href="#">Ivory Coast</a>	283	<a href="#">Spain</a>
57	<a href="#">Chile</a>	172	<a href="#">Japan</a>	291	<a href="#">Sweden</a>
62	<a href="#">Colombia</a>	180	<a href="#">Kosovo</a>	297	<a href="#">Switzerland</a>
69	<a href="#">Croatia</a>	182	<a href="#">Luxembourg</a>	303	<a href="#">Thailand</a>
75	<a href="#">Cyprus</a>	190	<a href="#">Mexico</a>	308	<a href="#">The Netherlands</a>
84	<a href="#">Czech Republic</a>	196	<a href="#">Morocco</a>	314	<a href="#">Türkiye</a>
91	<a href="#">Denmark</a>	203	<a href="#">Nigeria</a>	321	<a href="#">Ukraine</a>
98	<a href="#">Ecuador</a>	209	<a href="#">Norway</a>	327	<a href="#">United Kingdom</a>
103	<a href="#">Finland</a>	216	<a href="#">Panama</a>	335	<a href="#">Uruguay</a>
111	<a href="#">France</a>	221	<a href="#">Paraguay</a>	341	<a href="#">Contributors</a>
120	<a href="#">Germany</a>	228	<a href="#">Peru</a>		
125	<a href="#">Ghana</a>	234	<a href="#">Poland</a>		

# Introducing Deloitte Legal

Where legal meets business

Blending business experience and legal excellence  
we deliver **comprehensive solutions...**



**...designed to address the evolving needs of businesses**

We bring a global reach and collaborative mindset at a time of unprecedented change and transformation.



**...developed with a business-first approach and methodology**

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

Deloitte Legal professionals see the law as **empowering, not confining. We bring business solutions to legal issues and legal solutions to business issues. Plain and simple.**

## A different legal perspective

Traditional legal services provide event-based specialist advice. At Deloitte we seek out solutions aimed at delivering enduring business value. 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.



*Jurisdictional advisory, legal function strategy process and technology, and outsourced legal managed services*

As part of Deloitte, our legal service offering is inherently **broader, global, cross-functional, industry informed, technology enabled**, with a focus on doing and advising in our business solution centered approach.

# Overview

## A complex framework, a cross-jurisdictional approach

In today's digital age, data has emerged as a cornerstone asset for businesses across all industries and sizes.

Effective data governance, protection, security, and valorization are no longer optional but essential for driving innovation, enhancing decision-making, and gaining a competitive edge.

Beyond being a legal imperative in many jurisdictions, safeguarding data has become a strategic necessity. By mitigating risks and harnessing the potential of emerging technologies like artificial intelligence, organizations can unlock significant opportunities.

A deep understanding of the complex legal landscape is crucial to navigating this evolving data environment.

To address this need, Deloitte Legal initiated a cross-jurisdictional annual report in 2022 to track and analyze regulatory developments related to data across various jurisdictions.

The previous year's edition is accessible [here](#).

Deloitte colleagues from 50 jurisdictions contributed to this third edition, providing the latest legal developments in personal data protection, cybersecurity, and artificial intelligence.

The impact of these intricate and constantly evolving regulatory frameworks is increasingly profound for businesses of all sizes.

Any organization, while leveraging data and innovative technologies to drive innovation, must simultaneously navigate this complex legal landscape.

This report serves as a valuable resource for businesses seeking an international overview of:

- Recent developments: the most significant recent laws, regulations, guidelines, decisions, and sanctions in data protection, cybersecurity, and artificial intelligence; and
- Future trends: potential upcoming developments in these fields over the coming months.







## *Past*

Most relevant data protection, cybersecurity and AI updates of the last months

## *Future*

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

# National updates and developments



# Albania

## Contacts



**Ened Topi**

Senior Managing Associate, Deloitte Legal Albania  
[etopi@deloittece.com](mailto:etopi@deloittece.com)



**Jona Rapi**

Managing Associate, Deloitte Legal Albania  
[jrapi@deloittece.com](mailto:jrapi@deloittece.com)

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

## Recommendations on data protection

Throughout 2024, the Commissioner for the Right to Information and Protection of Personal Data (the Commissioner) issued nine recommendations concerning the protection of personal data. These recommendations were addressed to key controllers in the education, health, and real estate sectors, including the National Business Center (QKB) and the Independent Qualification Commission (KPK).

Considering these recommendations, controllers are required to:

- Carry out adequate processing of personal data;
- Collect, store, and publish personal data in accordance with its intended purpose;
- Map the premises that can be monitored by CCTV cameras;
- Respect the right to information for data subjects;
- Implement technical and organizational measures for the protection of personal data;
- Process data based on data categories, processes, and subjects' rights;
- Train employees who have access to and process personal data;
- Implement, maintain, and manage an Information Security Management System (ISMS);
- Develop relevant internal documents, specifically the Regulation "On the Protection, Processing, Storage, and Security of Personal Data" and the "Declaration of Confidentiality"; and
- Comply with the instructions issued by the Commissioner regarding the processing of data captured by video surveillance systems.

## Recommendations for the Independent Qualification Commission

The right of a party to access documentation and facts administered by the controller shall be regarded as the right to access personal data. The controller must provide any relevant information in the stored and processed form.

## Recommendations for large-scale processors

Based on their activities and the categories of data they process, these processors should enhance their internal technical and organizational measures to maintain a higher standard of data processing and invest in staff training.

## **"Is it forbidden (or not) by the legislation in force to place CCTV cameras in public pools/shared areas of a complex?"**

The Commissioner pointed out that *"Footage or images stored in the video-surveillance system (CCTV camera) shall be considered as "personal data," as information stored in these records can be used to directly identify individuals. To that end, the processing of this data must be carried out in accordance with legal requirements."*



## Publication of personal data on social platforms

In two recommendations addressed to educational institutions in Albania, regarding the publication of photos and videos on social networks, the Commissioner accentuated the importance of “written consent” relating to the concept of “personal data”.

Publication of personal data on social media platforms – specifically Facebook or Instagram – shall be considered as “processing.” As such, it is only legitimized if the data subject is aware of this fact and has given their written consent.

The controller is responsible for documenting this consent. Controllers shall provide complete information regarding the purpose and manner of processing personal data, the authorized data processors, the data retention period, security measures, and the rights of data subjects regarding access, correction, and removal of their information.

Data collected for each subject must include the category of subjects, information about their respective rights, time frames for data retention and processing, and information for processors regarding their responsibilities in the event of unauthorized dissemination.

## The Commissioner imposed a total fine of ALL 460,000 (approx. €46,000) on a telecommunications company for:

- Illegal collection and processing of personal data through CCTV cameras;
- Lack of transparency towards the subjects of personal data;
- Failure to inform the Commissioner about the activities carried out; and
- Failure to secure the collected data.

The processor is obliged to pay the fine, cease camera monitoring, destroy all data collected via the CCTV cameras, and document this process.

Moreover, one of the local education offices in Albania was fined ALL 180,000 by the Commissioner for failure to comply with data protection legal requirements. These requirements are more demanding for this subject, which is considered a “*large-scale data processor*” due to the category and volume of personal data it processes. The fine was imposed for:

- Non-compliance with the procedure for the destruction of documentation containing personal data;
- Lack of a technical and organizational structure for data protection; and
- Collection and processing of data by untrained personnel.

Other fines are lower in values, but for violations related to the failure of informing the Commissioner about installation of CCTV cameras, personal data processing, essential lack of “Regulation on Protection, Processing, Storage and Security of Personal Data” and “Declaration of Confidentiality”.



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

## Digital Albania

Starting in 2023, AI will be implemented, where possible, in electronic information and communication technology systems to enhance innovation in the digital economy (Law No. 43/2023 “On Electronic Governance”). Public services will soon be fully digitized, with AI integrated into these areas, which may help address issues of injustice and tax evasion.

In the same year, Albania became an associate member of the Digital Europe Programme 2021-2027. This will enable stakeholders from the public sector, private sector, and academia to participate in and benefit from EU projects focused on AI.

## AI in public services

AI is now a priority in government policies. In 2023, public institutions responsible for aligning with the EU ACQUIS piloted from August to December 2023, the use of AI in the legal approximation process.

Moreover, the Council of Ministers adopted two national strategies which aim to integrate and regulate the implementation and usage of AI in the country.

## Policy and regulatory developments since 2023

- Decision of Council of Ministers No. 479, dated 24 July 2024 “On the Approval of the Methodology Document and Technical Standards for the Use of Artificial Intelligence in the Republic of Albania”;
- Decision of Council of Ministers No. 161, dated 20 March 2024 “On the Approval of the Document on Priority Policies 2025-2027”; and
- National Strategy for Public Procurement.

## e-Albania virtual assistant

In alignment with the objectives set in the adopted strategies, the first version of the e-Albania virtual assistant was launched on 28 December 2023. This assistant automates responses and provides quick instructions for common questions regarding the platform’s 1,237 electronic services.

## Technical standards for the use of AI

Developers shall comply with the following risk classification of AI systems, before placing a system in the Albanian market (Methodology Document and Technical Standards):

- Unacceptable risk: AI systems incompatible with EU values and fundamental rights;
- High risk: AI systems used in critical infrastructure that may endanger life/health, educational and vocational training, access to education and career opportunities, product safety, employment management, essential services, law enforcement, migration management, administration of justice, and democratic processes;
- Limited risk: Systems with minimal risk but requiring some user awareness; or
- Minimal risk: AI systems that pose no risk to security, privacy, EU values, or fundamental human rights.



## Safety and robustness of AI systems

The Methodology Document and Technical Standards require AI systems to be developed and deployed in a way which ensures ethical and fair use, guided by ethical principles, organizational standards, and technical requirements. Throughout their life cycle, AI systems must adhere to these standards: (i) safe design and operating procedures; (ii) safe implementation; (iii) operation and maintenance; (iv) product testing and performance; (v) interface and networking; (vi) integrity; (vii) source of data; (viii) data management; (ix) training and testing of AI systems; (x) clear cybersecurity environment; and (xi) supply chain integrity.

## Ethical standards in AI development

AI systems are required to perform in accordance with these ethical standards: (i) proportionality and non-harm; (ii) safety and security; (iii) right to privacy and data protection; (iv) governance and collaboration; (v) responsibility and accountability; (vi) transparency and explainability; (vii) human oversight and determination; (viii) awareness and literacy; and (ix) fairness and non-discrimination.

## Design principles for AI systems

The Methodology Document foresees the following six design principles as an integral part of an AI system: (i) sustainable development, inclusive growth, and well-being; (ii) human rights and democratic values, including fairness and privacy; (iii) transparency and explainability; (iv) robustness, security, and safety; (v) risk management approach; and (vi) system accountability.

## Monitoring throughout the cycle

AI systems will be monitored throughout their life cycle to ensure compliance with regulatory requirements and existing legislation. The responsible authority in Albania will be the National Agency of Information Society AKSHI.

To that end, the Methodology Document stipulates that, development of AI in Albania should involve:

- Investment in AI research and development;
- Fostering an inclusive AI-enabled ecosystem;
- Shaping an interoperable governance and policy environment for AI;
- Building human capacity and preparing for the labor market; and
- International cooperation for trustworthy AI.

Last, but not the least, throughout their life cycle, AI systems should be:

- Trustworthy and reliable;
- Safe and resilient;
- Responsible and transparent; and
- Focused on privacy.

These ethical, technical, and organizational principles shall be integrated into the internal policies, guidelines, directives, and procedures of public institutions and private companies (Methodology Document and Technical Standards).

# ? What are the most relevant **cybersecurity updates?**

## National commitment on cybersecurity

In 2024, and after several cyberattacks that have seriously threatened information systems, Albania approved several important acts aimed at enhancing cybersecurity protection; which include the:

- National Security Strategy;
- Law No. 25/2024 “On Cyber Security”;
- Regulation “On the Cyber Incidents Classification”; and
- Regulation “On the Content and Method of Documenting Security Measures in Critical and Important Information Infrastructures”.

## National Security Strategy

The newly adopted National Security Strategy emphasizes enhancing the protection and cyber resilience of critical information infrastructure. This can be achieved by strengthening capacities through national and international cooperation.

## New law on cyber security

Starting in April 2024, new security measures were implemented to enhance the cybersecurity of networks and information systems (Law No. 25/2024). A crucial principle of this law is “*technological neutrality*,” which allows organizations the freedom to choose the most appropriate technology suited to their needs without being dependent on specific knowledge.

Additionally, the law defines cyber incidents and classifies cybersecurity measures into three categories: (i) precautionary measures; (ii) countermeasures and playbooks; and (iii) general protective measures. The relevant authority may update these security measures as needed to align with the latest technological developments, aiming to prevent and minimize the effects of cyber incidents on networks and information systems.

In the event of a cyber risk, the following measures should be considered: (i) network security; (ii) incident management; (iii) service continuity management; (iv) monitoring, auditing, and testing; and (v) compliance with national standards.

In the result of a cyber incident, authorities shall comply with the requirements of the new Regulation on Cyber Incidents Classification (2024) regarding the elements and format of reporting, as outlined by the reporting deadlines, and make sure to document and keep records for each cyber incident.





# What are the most relevant expected developments in data protection, AI and cybersecurity?

## Incorporation of European standards into national data protection law

In late 2024/early 2025, amendments to the existing law are expected to be finalized to align legislation with the Regulation (EU) 2016/679 and Directive (EU) 2016/680. This follows the conclusion of a public consultation on proposed changes to the existing data protection law, which took place in 2022.

Significant improvements in data protection are expected to be made particularly in the following areas:

- Enhancement of the right to information;
- Categorization of information in data processing scenarios;
- The right to request detailed blocking of processing;
- The right to be forgotten; and
- The right to data portability.

Additionally, genetic data, biometric data, and data on sexual orientation will be classified as “sensitive data.” The Commissioner is also expected to have increased obligations, particularly concerning the imposition of stricter administrative sanctions.

## Integration of AI in the e-procurement system

AI technologies and robotic processes will be integrated into the e-procurement system (as part of the National Strategy for Public Procurement) for the following activities:

- Contract value estimations;
- Market research;
- Drafting electronic specifications;
- Interfacing with other systems;
- Automating processes;
- Developing tendering procedures; and
- Selecting the best supplier/contractor for a tendering process.

The integration of AI in the electronic public procurement system aims to enhance transparency and integrity in the procurement and tendering process.



## AI in the legal approximation process

The implementation of AI in the legal approximation process (as part of Decision No. 161 “For the Approval of the Document on Priority Policies 2025-2027”) is expected to begin by early 2025.

Processes that might be automated include:

- Acts translation;
- Assessment of the impact of the EU acquis; and
- Gaps identification.

## National law and regulations on AI

In the near future, Albania is expected to adopt laws and regulations for domestic AI governance across specific industries and business sectors, with a strong focus on risk management plans. Additionally, dedicated training sessions will be provided for developers and deployers of AI systems.

Standards adopted by the government will incorporate best practices and high standards set by international organizations such as the US, EU, and OSCE (Organization for Security and Co-operation in Europe). Consequently, developers will be legally required to develop reliable, interoperable, and ethical AI. Specifically, they should comply with the following legal, technical and ethical requirements.

## Upcoming cybersecurity developments

The regulation “On the Method of Documentation and Implementation of Security Measures in Critical and Important Information Infrastructures ” is in full force since mid-2024 and it ensures compliance with and updates reflecting the requirements of the new law.

By the middle of 2025, the responsible authority for implementing and monitoring cybersecurity in Albania – the National Cyber Security Authority – will outline the next five-year National Cyber Security Strategy, which will be approved by the Council of Ministers by the end of that year.

# Argentina

## Contacts



**Eduardo Patricio Bonis**

Partner, Deloitte Legal Argentina

[ebonis@deloitte.com](mailto:ebonis@deloitte.com)



**José María Martín**

Senior Lawyer, Deloitte Legal Argentina

[josemartín@deloitte.com](mailto:josemartín@deloitte.com)

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

## **Argentine data protection regulations**

### **Agency for Access to Public Information**

In September 2016, the Law on Access to Public Information (Law No. 27.275) was enacted, which institutionalized the creation of the Agency for Access to Public Information (AAIP). This autonomous body acts as the enforcement authority for three key regulations: the Access to Public Information Law, the Do Not Call Registry Law (Law No. 26.951), and the Personal Data Protection Law (Law No. 25.326).

The AAIP plays an active role in promoting practices and regulations that improve the culture of personal data protection among the society. To this end, it conducts audits, inspections, and investigations. Under its jurisdiction, the National Database Registry has been established.

In 2022, the AAIP announced the intention of reforming the current Personal Data Protection Law and produced a draft bill that was then endorsed by the Executive Branch with minor adjustments. On 30 June 2023, the Executive Power sent Message 87/2023 with the Personal Data Protection Bill to the National Congress.

Even though this draft bill has not been treated yet (and most probably won't be treated by congress in 2024 and a new project would need to be presented), is an important precedent that evidence the intention to improve and update the data protection legal framework, since such draft bill follows the guidelines of the most recent personal data protection legislation, such as the UK's General Data Protection Regulation, Brazil's General Data Protection Law, and Ecuador's Organic Data Protection Law, among others.

Among the main proposed changes, it is worth mentioning:

- New definitions such as international data transfer, genetic data, and biometric data are included;

- Data subjects: Covering only individual's personal data, excluding information about legal entities, unlike the current regime that includes both cases;
- Extraterritorial application: Applying it to organizations outside Argentina that offer goods, services, or monitor the behavior of people in Argentina;
- Data processing principles: It introduces the principles of data minimization, accountability, recognized in the GDPR but not explicitly in the current Personal Data Protection Law (LPDP);
- Enhanced responsibility: Criteria for enhanced responsibility for handling sensitive data are included;
- Security breach notification: The obligation to notify the AAIP of security breaches that compromise personal data without undue delay and within 72 hours of becoming aware of such incidents is imposed;
- International data transfer: Specific requirements for the international transfer of data are established;
- Data subject rights: They are expanded, adding data portability, the right not to be subject to automated decisions, and to obtain the limitation of processing;
- Privacy Impact assessment: When the data controller considers carrying out a type of processing that implies a higher risk to the data subjects' rights, a privacy impact assessment must be conducted; and
- Database registry: The obligation to register databases before the AAIP is eliminated.





An important update came through the government's ratification of the Protocol amending Convention 108 (informally referred to as "Convention 108+"). This protocol recognizes data protection principles and provisions which are aligned to the GDPR, including the obligation to report data breaches.

Resolution 198/2023 of the AAIP recognized the standard contractual clauses (SCC) drafted by the Ibero-American Data Protection Network as a valid mechanism to transfer personal data to non-adequate jurisdictions.

In January 2024, the European Commission (EC) ruled that the adequacy decision of Argentina is still valid. Personal data transferred from the European Union to Argentina continues to benefit from adequate data protection safeguards.

In May 2024, Resolution 126/2024 of the AAIP amended the sanction regime for violations to the Personal Data Protection Law and the Do Not Call Registry Law.

# ? What are the most relevant **cybersecurity updates**?

## Cybersecurity in Argentina

### Legal developments

In terms of cybersecurity, Argentina has made great strides in the last decade. A milestone was reached in 2012 by means of Resolution 580/2011 of the Chief of the Cabinet of Ministers (*Jefatura de Gabinete de Ministros*), which created the National Program for the Protection of Critical Information Infrastructures and Cybersecurity within the scope of the National Office of Information Technologies of the Undersecretariat of Management Technologies of the Cabinet Secretariat of the Chief of Cabinet of Ministers.

The purpose of the national program was to promote the creation and adoption of a specific regulatory framework that promotes the identification and protection of strategic and critical infrastructures of the national public sector.

Subsequently, in 2019, Decree 480/2019 expanded the orbit of the Cybersecurity Committee. Later, the Government Secretariat for Modernization issued Resolution No. 829/2019 that created the National Cybersecurity Strategy.

It establishes the objectives of the strategy, which are: (i) awareness of the safe use of cyberspace; (ii) training and education in the safe use of cyberspace; (iii) development of the regulatory framework; (iv) strengthening of prevention, detection and response capacities; (v) protection and recovery of public sector information systems; (vi) promotion of the cybersecurity industry; (vii) international cooperation; and (viii) protection of critical national information infrastructures.

The latest advance in the matter was driven by the Ministry of Security of Argentina, by means of Resolution 914/2024 dated 12 September 2024, which created the "Cyber Synergy Center of Federal Police and Security Forces." The mission of this center is the analysis, investigation, and prevention of cybercrimes. It will be staffed by selected personnel from five federal forces, which will be authorized to provide support in cases involving cybercrimes. These forces are the Argentine Federal Police (PFA), the National Gendarmerie (GNA), the Airport Security Police (PSA), the Argentine Naval Prefecture (PNA), and the Federal Penitentiary Service (SPF).



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

## IA updates in Argentina

In Argentina, the developments in artificial intelligence (AI) from a legal perspective have been remarkable and have focused on establishing a regulatory and ethical framework for its development and use. Below is a summary of these advancements:

### Regulatory framework

Although there is no specific law on artificial intelligence, efforts are being made to develop a regulatory and ethical framework to guide the use and development of AI in the country. This includes the creation of guidelines and ethical principles to ensure that AI is used responsibly and safely.

### Personal Data Protection Law (Law 25.326)

This law also applies to the use of AI in Argentina, as it regulates the collection, storage, and processing of personal data, which are fundamental to many AI systems. The regulation seeks to ensure that the privacy rights of individuals are respected in the context of AI use.

### Government initiatives

The national government, through Administrative Decision 750/2023, has established an interministerial committee on artificial intelligence, aiming to address its advancements and applications in the economy. The objective is to design a comprehensive strategy for the implementation of AI in Argentina. This initiative seeks to facilitate more accurate diagnoses and advance the development of necessary regulatory frameworks to minimize the potential adverse impacts of AI.

A relevant update was made by Resolution No. 161/2023 of the AAIP, which approved the program for transparency and personal data protection in the use of artificial intelligence. In 2024, the AAPI published the “Guidelines for Public and Private Entities on Transparency and Personal Data Protection for Responsible Artificial Intelligence”, discussing the main issues and challenges surrounding AI and outlining recommendations applicable to the various stages of the AI system lifecycle.

### International collaboration

Argentina actively participates in international forums and organizations working on the regulation and ethical development of AI. This international collaboration seeks to align national policies with global best practices and promote the exchange of knowledge and experiences.

### Advisory Commission on Artificial Intelligence and Big Data

In 2019, the Advisory Commission on Artificial Intelligence and Big Data was created within the Ministry of Science, Technology, and Innovation. This commission aims to advise the government on policy and strategy formulation related to AI and big data.

### Legislative proposals under debate

There are several legislative proposals under debate in congress that seek to regulate specific aspects of AI, such as algorithm transparency, responsibility in the use of AI systems, and the protection of citizens' rights in relation to AI.

These developments demonstrate Argentina's commitment to establishing a legal and ethical framework that promotes the responsible development of artificial intelligence while protecting the rights and security of citizens. However, as with cybersecurity, it is essential that laws and policies continue to adapt as technology and its applications evolve.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Development prospects in Argentina

To align data processing standards and cybersecurity protections with international norms, significant efforts have been undertaken. In the realm of cybersecurity, training and awareness programs have been implemented for public officials, businesses, and citizens, with the aim of fostering a culture of cybersecurity. Additionally, Argentina has intensified its collaboration with international organizations and neighboring countries to enhance regional cybersecurity. This includes participation in international initiatives and agreements.

The Argentine government has launched several initiatives to promote the development and adoption of artificial intelligence. These initiatives include the creation of programs and policies to boost research and development in the field of AI, as well as to promote its use in key sectors such as health, education, and security.

These advancements reflect Argentina's growing commitment to addressing challenges in cybersecurity, data privacy, and AI through a robust legal framework and a coordinated national strategy. However, the digital environment is rapidly evolving, making it crucial for laws and policies to continuously adapt to new threats and vulnerabilities.

In the future, amendments to the Personal Data Protection Law are anticipated, aiming to align it with international standards and adapt it to emerging technologies, including references to cybersecurity and AI. Specific regulations are also expected to be enacted to govern the use of AI and the obligations of AI service providers. Regarding cybersecurity, it is likely that the regulatory framework will continue to progress towards harmonization with international standards. For instance, the draft reform of the Personal Data Protection Law incorporates concepts from the ISO 27001 standard, which pertains to cybersecurity.



# Australia

## Contacts



**Rachel Sciascia**

Partner, Deloitte Legal Australia  
[rsciascia@deloitte.com.au](mailto:rsciascia@deloitte.com.au)



**Celeste Bennett**

Director, Deloitte Legal Australia  
[cebennett@deloitte.com.au](mailto:cebennett@deloitte.com.au)

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

## The future of privacy: How the 2024 Privacy Act Amendment Bill strengthen data protection in Australia

The Privacy and Other Legislation Amendment Bill 2024, introduced on 12 September 2024, contains several pivotal changes aimed at strengthening privacy protections, including:

- **Doxing:** Making it a criminal offence to use a carriage service (e.g., by email, through the internet, phone calls or text messages) to release personal data in a menacing or harassing manner.
- **Serious invasions of privacy:** A statutory tort of invasion of privacy for intruding upon a person's seclusion (i.e., physically intruding on their space, or watching or recording their activities) or misusing information relating to that person, if they had a reasonable expectation of privacy and the invasion was serious and either intentional or reckless.
- **Automated decision-making:** Organizations with automated decision-making (ADM) systems using an individual's personal information that could significantly affect the individual's rights or interests must update their privacy policies to reflect the use of this program, types of personal information used and decisions the program can make.
- **Children's Online Privacy Code:** Mandating the Privacy Commissioner develop the Children's Online Privacy Code setting out how the Australian Privacy Principles (APPs) will apply to children's privacy and applying to social media services and internet services providers likely to be accessed by individuals under 18 years, and which are not providing a health service.

- **Reasonable steps obligations:** For entities that must comply with the APPs, the bill clarifies that reasonable steps an entity must take to protect personal information they hold from misuse, interference, loss, unauthorised access, modification or disclosure include technical and organisational measures. The Explanatory Memorandum for the bill identifies examples of organisational measures as steps, processes and actions that should be put in place (e.g., employee training, operating procedures and policies).

# ? What are the most relevant **cybersecurity updates?**

## **International cybersecurity guidance: ‘Choosing Secure and Verifiable Technologies’**

This guidance paper, released by the Australian Cyber Security Centre (ACSC) in partnership with the US, UK, Canada and New Zealand cybersecurity counterparts, is a non-binding roadmap, targeting entities manufacturing digital products and services and entities procuring and leveraging these products and services on ensuring how these products and services can be secure-by-design and secure-by-default.

This paper contains a two-stages approach for assessing security pre-purchase and post-purchase and from an internal procurement and external procurement perspective. While it emphasizes the importance of choosing secure and verifiable technologies and highlights the need for organizations to proactively integrate security considerations into their procurement processes to mitigate risks and reduce costs, it also assists manufacturers regarding the design of digital products and services to increase the development of secure technologies.

This paper is a framework to assist organizations in making informed, risk-based decisions. Recognizing the uniqueness of each organization, it encourages tailoring the procurement process to suit operational, and regional needs.

## **Countering foreign state information manipulation with the US**

On 5 August 2024, Australia entered into a Memorandum of Understanding (MOU) with the United States endorsing the US’s Framework to Counter Foreign State Information Manipulation.

The MOU, which has a four-year term, is non-binding and contains five action areas:

- **Strategies and actions:** Moving beyond ‘monitor and report’ approaches to developing strategies and implementing actions to counter the threat of foreign state information manipulation;
- **Governance structures:** Having designated governance structures and institutions to coordinate a national-level approach to counter these threats;
- **Human and technical capacity:** Maintaining threat awareness requires technical means and human capacity;
- **Supporting government initiatives:** Engaging civil society, independent media and academia to inform and support government initiatives countering foreign state information manipulation; and
- **International cooperation:** Information and capability shortfalls across partner nations can be addressed through multilateral organizations and plurilateral groupings leveraging international cooperation.

Australia has joined other countries in being a signatory to this MOU, with countries in various regions, including Europe, Africa, North America, and the Indo-Pacific having signed this MOU with the US.



## New mandatory directions for Commonwealth government entities

The Secretary of the Department of Home Affairs has introduced three mandatory directions under the Protective Security Policy Framework (PSPF) to enhance cybersecurity and combat foreign interference across Commonwealth government entities. These measures will influence how entities procure and manage technology assets and services.

The directions focus on three key areas:

- Managing Foreign Ownership, Control or Influence (FOCI) risks;
- Conducting technology stock takes; and
- Sharing cyberthreat intelligence.

The first direction mandates agencies to identify and manage FOCI risks in technology procurements, addressing concerns about foreign influence in government supply chains. By June 2025, all agencies must implement processes to manage these risks, which includes conducting a risk assessment of potential FOCI risks.

The second direction requires a stock take of all internet-facing technology assets by June 2025. Agencies must actively manage vulnerable technologies and develop risk management plans to address cybersecurity vulnerabilities and FOCI risks.

The third direction mandates agencies to participate in the Australian Signals Directorate's (ASD) Cyber Security Partnership Program and share threat intelligence with the ASD by July 2024.

Successful implementation will require a multidisciplinary approach, with agencies tailoring their efforts to their specific risk environments and technology supply chains.





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

## Australian government interim response relating to safe and responsible AI consultation

In January 2024, the Australian government published an interim response to the public consultation for 'Safe and Responsible AI in Australia'.

The interim response highlights that:

- **Legislative framework:** Australia's existing legislation does not prevent AI-facilitated harm before it occurs and does not prevent harm from deploying AI systems in high-risk legitimate settings and frontier AI models. Harm may also be increased due to the speed and scale of AI systems and this harm could potentially be irreparable; and
- **Regulation:** Consideration should be given to introducing mandatory obligations on entities developing or using high-risk AI systems, while not impeding use of low-risk AI. Further consideration will be given to how this can occur whether by existing laws or new approaches.

The Australian government has not identified how AI will be regulated, but has provided principles that will guide its response including:

- Adopting a risk-based approach, with a balanced and proportionate position which balances innovation and competition with protecting community interests;
- Being open in its engagement with experts and engaging with the public;
- Being a trusted international partner supporting 'global action to address AI risks'; and
- Placing 'people and communities at the center when developing and implementing its regulatory approaches.

## Established expert AI group

In February 2024, following the Australian government interim response, the Minister for Industry and Science announced establishment of a new Artificial Intelligence Expert Group. The group will provide advice to the Department of Industry, Science and Resources "on immediate work and transparency, testing and accountability, including options for AI guardrails in high-risk settings."

The group was only to be in place until 30 June 2024 and was subsequently extended to 30 September 2024. There is an intention to establish a permanent advisory body to provide AI expertise.

## Senate Select Committee

On 26 March 2024, the Senate Select Committee on Adopting Artificial Intelligence was established "to inquire into and report on the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia" and is due to present its report in November 2024.

## Responsible AI Index

The National Intelligence Centre in partnership with Fifth Quadrant released the Responsible AI Index in September 2024. This index provides insights as to how Australian organizations are adopting responsible AI practices.



## Proposal paper introducing mandatory guardrails

As part of broader agenda to promote safe and responsible use of AI in Australia, a proposal paper introducing mandatory guardrails for AI in high-risk settings was introduced on 5 September 2024.

The proposal paper sets out:

- **High-risk AI:** A proposed definition of high-risk AI;
- **Mandatory guardrails:** 10 proposed mandatory guardrails around the development and deployment of AI in high-risk settings; and
- **Regulatory options:** Regulatory options for mandating these guardrails (e.g., adapting existing regulatory legislation or creating new frameworks etc.).

## Voluntary AI Safety Standards

The 'Voluntary AI Safety Standard' was introduced on 5 September 2024 as part of the broader agenda to promote safe and responsible use of AI in Australia.

The standard contains 10 guardrails:

- Nine of which align closely with the mandatory guardrails proposed above; and
- Which comply also with international standards.

The guardrails cover AI accountability, risk management, testing, human intervention in AI, disclosing AI usage to end users, providing processes for users to challenge AI outcomes, transparency, record keeping and stakeholder engagement.

## National framework for assurance of AI in government

The 'National framework for the assurance of artificial intelligence in government' was released by the Australian government in June 2024. This framework, based on Australia's AI Ethics Principles, provide a nationally consistent approach for AI assurance and ensuring safe and ethical use of AI across all levels of Australian government and aligns with global AI safety and responsibility initiatives and strategies.

The framework aims to enhance public confidence and trust in government use of AI with practical guidance for designing and using AI technology and in the assessing of risks and implementation of mitigation strategies, while allowing for governments to develop their own policies and guidelines.

## Policy for responsible use of AI in government

With the exception of national security agencies, Australian government agencies began implementing the 'Policy for the responsible use of AI in government' from 1 September 2024.

Designed with flexibility in mind, the policy seeks to create a coordinated approach to AI within the Australian public service, by establishing minimum requirements for governance arrangements relating to AI and agencies publishing statements about their approach to and use of AI and recommendations for consideration such as annual reviews.

The policy aims to foster a unified, responsible approach to AI in the Australian public service, balancing innovation and adoption with public trust and safety.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Copyright and Artificial Intelligence Reference Group

In December 2023, the Australian government announced it was establishing the Copyright and Artificial Intelligence Reference Group to “better prepare for future copyright challenges emerging from AI”, and enable engagement, sharing of information and discussions.

The reference group is expected to advise the government on key policies, gaps at the intersection of AI and copyright, and possible solutions. However, at present the reference group’s focus is AI systems’ use of copyright material as inputs. Other potential issues that may be explored relate to AI outputs such as copyright infringement in these outputs and the application of copyright to these outputs.

## Australian privacy regulator priorities

The Office of the Australian Information Commissioner have released its priorities for 2024 which include a focus on:

- **Emerging technologies:** Emerging technologies aligning with community expectations and comply requirements and targeting current and emerging harm;
- **Digital economy:** Promoting a “privacy-protecting digital economy” through compliance and supporting entities with the Notifiable Data Breaches scheme, digital ID system (which allows Australians to verify their entity online) and continuing with the consumer data rights co-regulation;
- **Open government:** Promoting timely access and proactive publication of government information; and
- **Privacy laws:** Strengthening and enforcing personal information protections and contributing to privacy law reform.

# Austria

## Contacts



**Sascha Jung**

Partner, Jank Weiler Operenyi Rechtsanwälte, Deloitte Legal Austria  
[s.jung@jankweiler.at](mailto:s.jung@jankweiler.at)



**Christian Kern**

Senior Manager, Jank Weiler Operenyi Rechtsanwälte, Deloitte Legal Austria  
[c.kern@jankweiler.at](mailto:c.kern@jankweiler.at)



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

## Legislation

### Informationsfreiheitsgesetz – IFG

Austria is one of the last countries in Europe to have transitioned from a constitutionally enshrined principle of official secrecy to a system of freedom of information. The new Federal Act on Access to Information (Freedom of Information Act – IFG, Änderung des Bundes-Verfassungsgesetzes und Informationsfreiheitsgesetz BGBl I 2024/5) will largely come into force on 1 September 2025. In this context the practical application of data protection law will face new challenges.

## Legislation

### New national legislation on media privilege adopted; amendments of the BAO/MPG 2021

After the Austrian Constitutional Court ruled at the end of 2022 that the previous regulation was unconstitutional (ruling of 14 December 2022, G 287/2022, among others), the Austrian legislature enacted a new national law on media privilege to comply with the Constitutional Court decision (§ 9 DSG, BGBl I 62/2024; which has been in force since 1 July 2024).

Furthermore, recent amendments to the Federal Fiscal Code (Bundesabgabenordnung, BAO, with BGBl I 2019/103) and the national Medical Devices Act (Medizinproduktegesetz 2021 - MPG, BGBl I 122/2021) are representative of many other legislative changes in Austrian law.

With the experience gained since the GDPR came into force, the legislator continues to use every opportunity to use national substantive laws to fill the opening clauses of the GDPR as meaningfully as possible – at the same time, of course, this also creates an additional need for advice.

# ? What are the most relevant **cybersecurity updates?**

## Implementation of NIS2

### NISG 2024 – “Please wait!”

Like some other European member states, Austria is also late in implementing the NIS2 Directive.

The exact date of implementation in Austria depends on the formation of a government and the parliamentary legislative process and is currently still open.

A draft law on the NISG 2024 (Netz- und Informationssicherheitsgesetz 2024) is currently on the table (in the version of the motion for an initiative of 13 June 2024), which has already been discussed in parliament but failed to obtain the necessary two-thirds majority and was therefore not adopted.

## DORA enforcement law

### First ministerial draft

The DORA Implementation Act is intended to clarify the following:

- Scope of application of DORA with regard to national financial undertakings (credit institutions, investment firms, insurance undertakings, payment institutions, etc.);
- Definition of the Financial Market Authority’s (FMA) supervisory and sanctioning powers for the effective enforcement of DORA;
- Rules on extended testing of financial undertakings; and
- Penal provisions.

For financial undertakings, the FMA is the competent authority for supervising compliance with the DORA (however, for credit institutions classified as significant, the European Central Bank performs this task).

Administrative fines of up to €150,000 are planned for natural persons and of up to €500,000 or up to 1% of the total annual net turnover (whichever is higher) for legal entities (Sections 6 and 7 of the draft). In addition to these fines, the FMA may also – as already known from the various supervisory laws – publish the imposed administrative penalties and the companies concerned on its website (“naming and shaming”). Penalties may be imposed for a variety of violations of the DORA, including failure to report ICT-related incidents and cyberthreats, failure to conduct regular testing, failure to manage ICT third-party risk, and failure to have contractual agreements with the ICT third-party service provider that comply with Article 30 DORA.

# Belgium

## Contacts



**Matthias Vierstraete**

Partner, Deloitte Legal Belgium

[mvierstraete@deloitte.com](mailto:mvierstraete@deloitte.com)



**Julie Van Com**

Managing Associate, Deloitte Legal Belgium

[jvancom@deloitte.com](mailto:jvancom@deloitte.com)

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

## **Framework for settlements by the Belgian Data Protection Authority (hereafter the DPA or Belgian DPA)**

### Settlement framework Belgian DPA

The Belgian DPA has introduced a framework for settlements based on their prerogative to conclude settlements established in Articles 95 and 100 of the Law of 3 December 2017 regarding the establishment of the DPA. The framework aims to provide insights to the public, and in particular to parties involved in proceedings before the Disputes Chamber, related to the settlement procedure before the Dispute Chamber of the DPA. In this framework, the DPA emphasizes that it has full competence and an active role to conclude settlements and that said settlements fall under a sui-generis statute. Furthermore, settlements can be concluded at any time during a procedure.

Further, the DPA points out to several advantages of the settlement framework, for instance, settlements:

- Enable that solutions for problematic issues are found more quickly;
- Imply interaction with the defendant to find appropriate and concrete solutions;
- Result in improved legal certainty and procedural efficiency; and
- Will mean less dismissal of cases and more satisfaction of grievances from plaintiffs.

The second chapter of the framework outlines some procedural elements:

- The settlement exists between the defendant and the DPA, the plaintiff is not a party to the final settlement but can comment in writing on the settlement offer;

- In itself, the settlement doesn't entail an admission of wrongdoing, it does, however, entail a confirmation of the facts by the parties;
- The settlement is confirmed by a settlement decision of the DPA;
- The settlement is subject to a deadline. If it is not reached within this period (or after an extension) the case will continue; and
- A failed settlement doesn't have any effect on future prospects of the case.

## **CJEU takes stance in the IAB Europe case C-604/22 and largely confirms its previous decision**

### **Extension of scope of “personal data” and clarification of the concept “joint controller”** CJEU ruling and Belgian DPA communication

IAB Europe (hereafter IAB) is an association of digital advertising undertakings which developed a well-known mechanism facilitating the management of users' preferences for online personalized advertising. Most importantly, the IAB created the Transparency and Consent Framework (TCF) which regulates how advertisers should use the real-time-bidding system, a system used for selling advertising space on the internet. Through this system, advertisers bid on the features of the user. Processing of personal data takes place through the consent of the user and the associated “TC String” created, which includes the personal data of the users. The DPA qualified this TC String as personal data. Furthermore, the DPA decided that IAB was a joint controller under the GDPR. The DPA's decision in 2022 held IAB liable for a variety of GDPR infringements and imposed a fine of €250,000. IAB however, appealed the decision, after which the Market Court posed two preliminary questions to the CJEU.



The CJEU held the following: *"the TC String constitutes personal data where those data may, by reasonable means, be associated with an identifier (including the IP address)."* In this case, it could be used to identify a natural person, the CJEU also reiterated that it is not necessary in this context that all identifiers are held by one controller.

The CJEU also ruled the following: *"IAB Europe can be deemed a joint controller with its members if it influences the personal data processing for its own purposes, and determines, jointly with its members, the purposes and means of such processing, which is up to the Belgian Court of Appeal to verify."*, such joint controllership is thus not automatic but should be considered on a case-to-case basis.

The Market Court will now rule on the appeal lodged by IAB, as well as by the complainants in the case, taking into account the answers provided to its preliminary questions by the CJEU.

## The DPA's fight on cookies

### NOYB vs. the Belgian media landscape

In 2023, the non-profit organization NOYB lodged several complaints with the Belgian DPA against major Belgian news sites.

The DPA has adopted settlement decisions in a number of cases against Belgian major news sites, namely, the [De Tijd](#) case (decision 159-2023), the [La Libre/dhnet](#) case (decision 160-2023), and the [VRT](#) case (decision 164-2023). All three cases were initiated by NOYB, filing complaints regarding cookie banners using dark patterns and with regard to non-compliant cookie banners. The DPA largely agreed with these complaints, however, it opted to pursue a settlement with the accused media companies, rather than pursuing a normal procedure.

An important note in this context is the focus on imposing purely actionable measures rather than imposing fines or monetary sanctions, which are also possible in the context of a settlement procedure.

However, other defendants weren't as cooperative with the DPA. For instance, the [Mediahuis](#) case (decision 113-2024) asked for certain adjustments in the context of the settlement proposal, nonetheless, the DPA refused and even withdrew the settlement proposal as a whole. Subsequently, Mediahuis was held liable for non-compliance with GDPR due to multiple issues with their cookie banner and their defiance in regularizing the banners in the context of the settlement negotiations. Regularizing obligations were imposed by the DPA and linked to a penalty to guarantee swift compliance.

Nevertheless, NOYB wasn't always this successful in forcing websites to become GDPR-complaint with regards to cookie banners. In their fight for cookie compliance, NOYB started sending pre-trial letters in 2021 and laid down over 200 complaints across European Data Protection Authorities.

However, some of these cases were started by NOYB employees or interns who had to actively search for non-compliant cookie banners and subsequently gave the procedural mandate to NOYB ([Article 80 GDPR](#)). As a result, the DPA considers the mandate based on Article 80(1) GDPR a fictitious mandate and considers it invalid. Rather classifying NOYB as a body under Article 80(2) GDPR.

Member states, however, have the prerogative to decide whether to implement Article 80(2) GDPR or not, Belgium has decided not to transpose said article. The DPA therefore decides that NOYB doesn't have standing nor the necessary interest under Article 80(2) to be able to lodge a complaint and therefore decided to dismiss the case.

## **Decision 169-2023: Conviction of the Roman-Catholic Church for failing to abide by a deletion request from the baptismal register, based on Article 17 GDPR**

### [DPA decision](#)

In this case, the plaintiff requested to be removed from the baptismal register in Ghent (both from physical and non-physical copies of the register). The plaintiff had been introduced in said register as a minor who had no choice in being baptized and therefore being included in the register of the Roman-Catholic Church.

The DPA held that the Roman-Catholic Church couldn't use legitimate interest as a legal basis nor could it use any of the exceptions in Article 9 as they processed sensitive data, namely religious beliefs, in the context of the baptismal register.

The DPA therefore imposed corrective measures to delete the plaintiff from the register and to bring the overall processing activities of the diocese in line with the GDPR.

# ? What are the most relevant **cybersecurity updates**?

## **Law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security (hereafter: NIS2 law)/NIS2 Royal Decree**

[NIS2 law adoption](#) and [NIS2 Royal Decree adoption](#)

In April 2024, Belgium became the first member state to transpose the NIS2 Directive. The federal government designated the Centre for Cybersecurity Belgium (CCB) as the competent authority regarding NIS2 introduction and enforcement.

The CCB has released a series of articles outlining the scope of NIS2, explaining who has to abide by which set of obligations, explaining the notification obligation, administrative measures, and finally also guidance on the necessary cybersecurity measures.

The NIS2 Royal Decree exhausts certain prerogatives of member states with regards to the NIS2 adoption. Firstly, it establishes the CCB as the national cybersecurity authority and the national cybersecurity incident response team (CSIRT). The decree also establishes which sectoral authorities will support the CCB, in most cases the CCB will be assisted in their tasks by the relevant ministerial administration.

The NIS2 Royal Decree establishes a framework for the regular conformity assessment procedures (amongst others the Cyberfundamentals Framework or CyFun) and associated reference frameworks which can be used. Most importantly the decree lays down the conditions to be accredited as a conformity assessment body (CAB).

## **The Cyberfundamentals Framework**

<https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework>

The Cyberfundamentals Framework (CyFun) is a framework created by the CCB to address the 10 Cybersecurity measures established in Article 21(2) NIS2 Directive and the vulnerability disclosure mechanism from Article 12 of the Directive.

The CyFun framework is based on four widely recognized cybersecurity frameworks, namely, ISO 27001/27002, NIST CSF, CIS Controls and IEC 62443. However, in Belgium, CyFun and ISO 27001 are the only two accepted reference frameworks for certification under the NIS2 Royal Decree.

The CyFun framework aims to improve cybersecurity and resilience in Belgium as a whole, it therefore doesn't merely focus on entities qualifying as "important" or "essential" under NIS2 but also provides guidance for micro-organizations or organizations with limited technical knowledge and all enterprises in general. However, extensive guides with specific rules of 60+ pages are introduced for "important" and "essential" entities.

The current certification mechanism under the CyFun framework starts with a CyFun self-assessment tool and guidance on corrective measures that need to be taken. Secondly, the entity must choose an authorized CAB who will assess the self-assessment and implementation of the cybersecurity measures. Once approved by the CAB, an organization can request the CyFun label on the "Safeonweb@work" portal, created by the CCB.

Consequently, the CCB also adopted the conditions, clarifications and overall guidance to be recognized as a conformity assessment body, so-called accreditation, in line with EU Regulation 765/2008, the NIS2 law and the NIS2 Royal Decree. An important note is that accreditation must be done through the national accreditation body – BELAC.

## The CCB introduces technical guidelines for the prevention and protection against DDoS cyberattacks

### [CCB technical guidelines DDOS protection and prevention](#)

The CCB published technical guidelines on Distributed Denial of Service (DDoS) protection and prevention. In a DDoS attack, a network website is overloaded by a botnet that simultaneously sends requests to the victim. The result may be that the availability of a service can no longer be guaranteed and will be unavailable.

It is important to note that these guidelines were published amidst the 2024 election campaign to encourage all relevant stakeholders to take the necessary preventive measures to guarantee fair and democratic elections in Belgium without any outside intervention.

The document establishes the different types of DDoS attacks and the reasoning behind such attacks. The CCB also establishes proactive measures which organizations can take and, moreover, mitigation measures in case of DDoS attacks.

To conclude, the guidelines provide a proactive checklist and a summary of incident response steps, both technical as non-technical, for mitigation after DDoS attacks.

## More than 10 million suspicious messages sent to Safeonweb

### [CCB announcement](#)

Safeonweb is the web portal created by the CCB to raise awareness and to bridge the technical knowledge with the needs of the public. 2023 was a successful year for the platform as the number of Belgians connecting with the platform and even actively sending suspicious messages had risen to 28%. This also becomes clear from the 10 million of messages sent to [suspicious@safeonweb.be](mailto:suspicious@safeonweb.be).

These messages are essential for the CCB and the Belgian Anti-Phishing Shield. The CCB analyzes the messages it receives and in the event it determines it relates to malicious websites, the CCB takes action by blocking the website, URL or attachment and users get redirected to a warning website.

In this context, the CCB also introduces some red flags of phishing messages which are used in practice but also warns for a new form of phishing, namely “quishing”. Quishing is the phenomenon of using QR-codes to redirect users to a suspicious website. Other phishing trends have largely stayed the same.





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

## **Flemish AI-strategy and guidelines on the use publicly accessible Generative AI tools**

[Vlaamse AI Strategy](#) and [Guidelines](#)

In the context of testing Copilot in Flemish administrations, the Flemish government has adopted two key documents with the aim of establishing a framework for the use of Generative AI, including Copilot. The first document is the Flemish AI strategy, which introduces the key principles that should be taken into account when using AI as a, or within a, Flemish administration. The second document, namely the guidelines on the use of publicly accessible Generative AI tools, focuses on implementation in practice by government officials.

The Flemish AI strategy largely follows the principles laid out in the AI Act with one notable addition. The principles established in the strategy are as follows:

- Democracy and rule of law;
- Trustworthy AI;
- Human-centered AI;
- Increase AI awareness;
- Correct data use and management; and
- Sustainability.

To quickly zoom in on sustainability as an additional principle, it is necessary to establish that the notion of sustainability in the AI Act refers to AI for sustainability as opposed to the sustainability within the Flemish AI strategy which refers to the need for AI to be sustainable on an environmental and human rights level.

To put these principles into practice, the Flemish government adopted the guidelines which include chapters on GenAI, the associated risks, the reasoning for the new guidelines, a list with GenAI tools that government officials can use and prompt-crafting tips and tricks, but, most importantly, guidelines on safe use and examples of (in)appropriate use of GenAI.

## **Charter for the use of AI by government administrations**

### **Introduced by the federal government**

[AI use charter for government administrations](#)

At first glance, this charter describes how AI is used within government administrations. It is intended as an information notice towards all citizens and to inform them on which values are being protected when using AI in the provision of government services. Furthermore, the charter is applicable to all AI systems and not only publicly accessible tools.

The charter establishes a set of commitments to citizens and explicit implementation measures, while these precede the AI Act, the charter is in line with the AI Act and the GDPR.

## **The advisory committee on ethics and law in the federal government**

[AI4Belgium Ethics and law announcement](#)

The advisory committee was introduced by Royal Decree with the goal of translating the existing rules, guidelines and ethical considerations to a government context. More concretely, the committee will advise governments and administrations on how to adopt AI in an ethical and lawful manner.

A similar role already exists for the private sector, namely, the Committee AI4Belgium on Ethics and Law. It is therefore logical that the advisory for the public sector resides within the same framework to draw from their expertise.

To a certain degree this might seem as overkill as the AI Act and Council of Europe Framework Convention on artificial intelligence and human rights, democracy and the rule of law, will already introduce a comprehensive set of rules and principles, these national institutions can go one step further and take into account local priorities, preferences and customs and provide tailored advice with understanding of the local context, especially in the public sector. The advisory committee itself is made up with philosophical experts, lawyers and data scientists.

## Artificial intelligence systems and the GDPR from a data protection perspective

### Information brochure published by the General Secretariat of the DPA

[AI brochure by the Belgian DPA](#)

The Belgian DPA published an information brochure related to quick developments accompanied by the increased use of AI systems. It also emphasizes the importance of GDPR for the correct and lawful implementation of AI, even within the European Union where the AI Act has led the public and legal debate.

This information brochure aims to educate a broad audience, including legal professionals, DPOs, business analysts, and technically-minded individuals, about the complementary relationship between the GDPR and the AI Act. It also aims to clarify and delineate these complementing obligations for use in practice.

It is important in this context to bridge the gap between legal obligations and technical implementation. Both legal professionals as individuals with technical expertise are key actors in this process.

The first chapter introduces the concepts of an AI system and provides some examples such as automated spam filters, recommendation systems on streaming services, virtual assistants and AI-powered medical imaging analysis.

The second chapter elaborates on AI by linking and integrating the obligations under the GDPR with those under the AI Act. For instance, as regards the principles under the GDPR it mentions:

#### Lawful, fair, and transparent processing

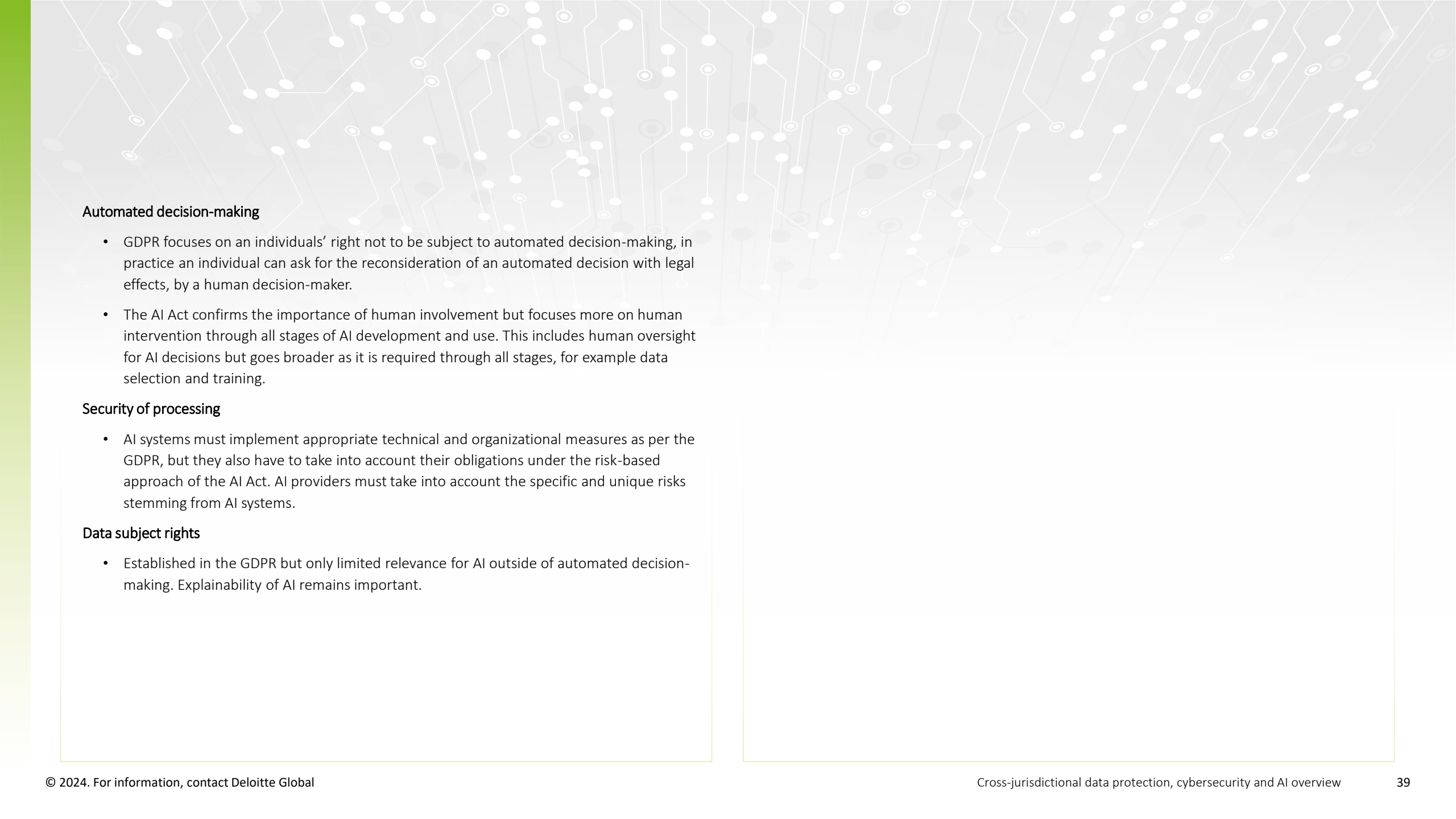
- Lawful processing: Article 6 GDPR is also applicable to processing of personal data by or in the context of AI-systems.

#### Purpose limitation and data minimization

- Articles 5(1)(b) and 5(1)(c) GDPR must be respected in the context of AI systems by ensuring that AI systems don't process personal data beyond their intended purpose or collect an excessive amount of data, the AI Act strengthens these provisions through the need for well defined purposes for high-risk systems.

#### Purpose limitation and data minimization

- The AI Act builds on the principle of data accuracy by obliging providers of high-risk AI systems to use high quality data to prevent biased and discriminatory outcomes.



### Automated decision-making

- GDPR focuses on an individuals' right not to be subject to automated decision-making, in practice an individual can ask for the reconsideration of an automated decision with legal effects, by a human decision-maker.
- The AI Act confirms the importance of human involvement but focuses more on human intervention through all stages of AI development and use. This includes human oversight for AI decisions but goes broader as it is required through all stages, for example data selection and training.

### Security of processing

- AI systems must implement appropriate technical and organizational measures as per the GDPR, but they also have to take into account their obligations under the risk-based approach of the AI Act. AI providers must take into account the specific and unique risks stemming from AI systems.

### Data subject rights

- Established in the GDPR but only limited relevance for AI outside of automated decision-making. Explainability of AI remains important.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Enforcement focus for the Belgian Data Protection Authority and organizational changes

[A new chapter for the Belgian DPA](#) and [Rules of internal order](#)

The Belgian DPA has delivered on its promise at the end of 2023 to crack down on cookie enforcement, not only through the cases mentioned in the previous slides, but also through establishing guidelines and cookie checklists.

Following internal restructuring in 2023 which resulted in a complete executive committee, the DPA underwent further organizational change in 2024, the amended law on the organization of the DPA entered into force on 1 June 2024. The DPA has taken this opportunity to implement a new document on internal regulations.

Some key takeaways from these new instruments are:

- These new rules are only applicable to cases submitted after 1 June 2024;
- The streamlining of certain procedures:
  - Empowering the “First Line Services” to realize mediations for more simple cases;
  - Updating the procedure before the DPA’s Dispute Chamber to ensure legal certainty and ensure the course of the procedure is as swift as possible until the moment of dismissal or implementation; and
  - New tasks and procedural rules for the authorization and advisory service.
- The Executive Committee is empowered with a more active and coordinating role to prioritize internal priorities and cooperation between its services; and
- Access to a set list of experts to assist the DPA throughout their activities.

## Centre of Cybersecurity Belgium strategy

### Going beyond NIS2

<https://ccb.belgium.be/en/organisation>

The CCB was a key driver behind the progress made regarding NIS2 during the Belgian European Presidency. Not unexpectedly as the CCB has been a very active administration in Belgium, pushing Belgium to top five in the UN Global Cybersecurity Index.

At the end of 2023, the CCB had identified the following aspects as policy goals and aims to build on these through 2024 and 2025:

- Establishing the Cyberfundamentals Framework (see above);
- Expanding Safeonweb@work – a tool for organizations to proactively implement measures to mitigate cybersecurity risks;
- Safeonweb browser extension – developed for both citizens and organizations, the browser extension provides information on whether the website’s owner identity has been properly validated;
- Raising awareness around phishing (see above) – expanding the Belgian Anti-Phishing Shield;
- Increase active cyber protection through spear warnings;
- Raise awareness around cybersecurity in the context of artificial intelligence; and
- Continue the fight against ransomware and DDoS attacks.

Finally, the implementation of NIS2 has become a top priority very quickly.



## Federal and regional cooperation for implementation of the AI Act

### The difficult Belgian federal landscape

As established above, both on the federal and regional level, there are many AI initiatives taken already. Ranging from investment schemes and use in administrations to establishing regulatory and ethical frameworks.

As governments in Belgium start seizing competence and exhausting their prerogatives in a context without the AI Act fully applicable, it will be interesting to see how this all-encompassing regulation will impact these competences. Especially when, under the AI Act a specific authority will have to be established or awarded competence to enforce the AI Act.

Logically speaking this authority will be set up on a federal level, as has happened in the context of GDPR (i.e.; the DPA). But this will not necessarily prevent regional authorities from setting up their own body, enforcing the same rules and seizing competence where possible within their prerogatives.

A short overview of current administrations with specific AI competences:

#### AI4Belgium

- A federal administration residing under federal public service policy and support;
- Active in AI ethical and legal issues; and
- Advisory body for the federal government and the private sector.

#### AI Centre of Expertise

- A Flemish administration operating under the Digital Flanders Authority; and
- Focuses on ethical principles and guidelines within Flemish administrations

#### Digitalwallonia4.ai

- Residing under Digital Wallonia; and
- Focuses on the development of AI and its role in the economy within the region by supporting it through subsidies and accelerators

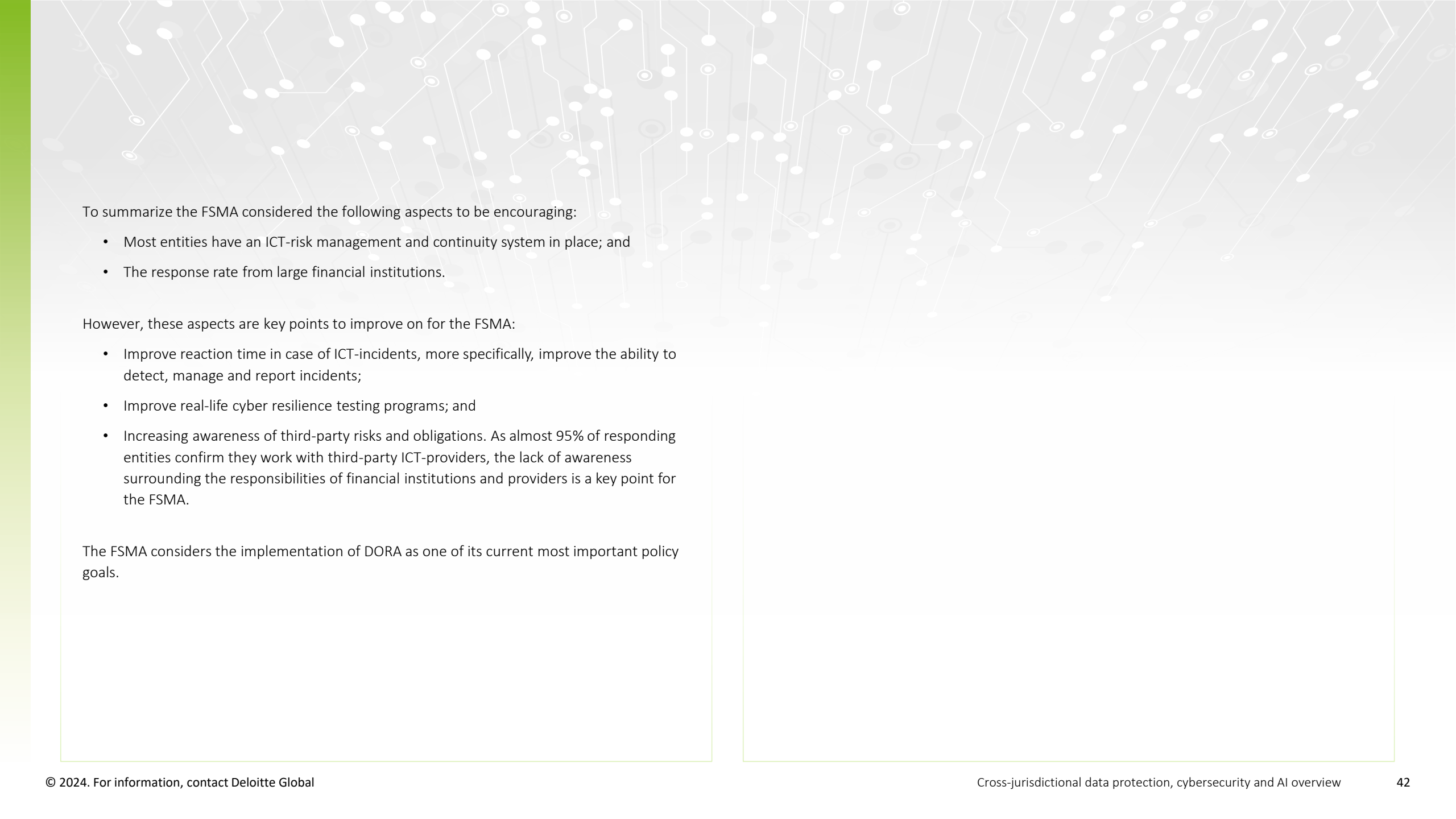
## Implementation of DORA regulation

### Awareness campaign on DORA regulation for financial sector

#### [FSMA: DORA implementation update](#)

In February 2024, the FSMA, the Belgian Financial Services and Markets Authority, tried to raise awareness around the Digital Operation Resilience Act (DORA) for the financial sector. After a thorough round of surveys, the FSMA concluded that, in general, financial services were underprepared and underfunded to tackle the regulatory obligations set out in DORA.

The FSMA ran a five-week survey in which half of the targeted entities responded. While this is an admirable response rate, the lack of response from certain sectors also worried the FSMA as there is currently no way to check whether or not these sectors and their associated organizations are prepared, furthermore, such lack of response could be interpreted as a lack of preparation. Two of these sectors were insurance and re-assurance brokers and crowdfunding platforms.



To summarize the FSMA considered the following aspects to be encouraging:

- Most entities have an ICT-risk management and continuity system in place; and
- The response rate from large financial institutions.

However, these aspects are key points to improve on for the FSMA:

- Improve reaction time in case of ICT-incidents, more specifically, improve the ability to detect, manage and report incidents;
- Improve real-life cyber resilience testing programs; and
- Increasing awareness of third-party risks and obligations. As almost 95% of responding entities confirm they work with third-party ICT-providers, the lack of awareness surrounding the responsibilities of financial institutions and providers is a key point for the FSMA.

The FSMA considers the implementation of DORA as one of its current most important policy goals.

# Bulgaria

## Contacts



**Miglena Micheva**

Senior Managing Associate, Deloitte Legal Bulgaria

[mmicheva@deloittece.com](mailto:mmicheva@deloittece.com)



**Irena Koleva**

Senior Associate, Deloitte Legal Bulgaria

[ikoleva@deloittece.com](mailto:ikoleva@deloittece.com)

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

## **Opinions of the Bulgarian Commission for Personal Data Protection**

### **Opinion on the notification by phone and email about the upcoming expiration of the validity period of identity documents**

The Bulgarian Commission for Personal Data Protection (CPDP) issued an [Opinion № ПНМД-01-88/2024](#) clarifying the possibility for the Bulgarian Ministry of Interior to use the collected personal data of citizens for the purpose of sending notifications for upcoming expiration of identity documents. Pursuant to the opinion, the telephone numbers of Bulgarian citizens collected through the application for the issuance of identity documents may be processed for the purpose of sending a notification for the forthcoming expiration of the validity of the identity documents and there is no need to make legislative changes. On the other hand, the Bulgarian regulator stated that the Ministry of Interior cannot use the emails collected from the application for issuance an identity document for the purpose of sending notifications for expiration without introducing legislative changes. In addition, the CPDP provided additional instructions regarding the obligations under the data protection legislation of the Minister of Interior as a data controller.

### **Opinion on processing of personal data contained in acts subject to promulgation in the "State Gazette"**

The CPDP issued an [Opinion № ПНМД-01-39/2024](#) regarding the promulgation of acts containing personal data in the State Gazette. The necessity of the adoption of the opinion has arisen from litigation initiated by a citizen whose data was published in an edition of the Bulgarian State Gazette. Pursuant to the opinion of the CPDP, legislative changes are necessary to explicitly oblige the senders of documents/acts for promulgation to erase the personal data contained in them, which are not relevant to the specific purposes of the promulgation.

Moreover, it's stipulated that the Bulgarian National Assembly should introduce temporary measures that reflect the factual relations and the necessity that State Gazette performs its activity in accordance with the provisions of the GDPR.

## **Methodological instructions issued by the Commission for Personal Data Protection**

In December 2024, the CPDP published its methodological instructions to the obliged entities under the Bulgarian Act on the Protection of Persons Who Report or Publicly Disclose Information on Breaches (Whistleblower Protection Act; the Act):

- [Methodological Instructions No 1](#) for Receiving, Registering and Considering Reports Received with Entities Obligated under the Act on the Protection of Persons Who Report or Publicly Disclose Information on Breaches; and
- [Methodological instructions No 2](#) regarding the Submission to the Commission for the Personal Data Protection of the Necessary Statistical information under the Act on the Protection of Persons Who Report or Publicly Disclose Information on Breaches.

The purpose of the methodological instructions are to support the activities of the obliged entities under the act and the employees/units designated by them, by establishing uniform rules and criteria in the implementation of the functions of receiving, registering and considering reports received through an internal reporting channel.





## Requests for preliminary rulings

In 2024, Bulgarian courts submitted requests for preliminary rulings to the Court of Justice of the European Union (CJEU) in the area of personal data protection, which are still in progress:

- [Case C-312/24](#) concerning various matters including the interpretation of the right to be forgotten in the specific case; and
- [Case C-541/24](#) whereby the proceedings stemmed from a lawyer's request to access case files without being an authorized representative of any of the parties or being a party to that case.

# ? What are the most relevant **cybersecurity updates**?

## **Amendments to the Cybersecurity Act transposing NIS2 Directive**

On 4 July 2024, the Minister of e-Government proposed a bill for amendment to the Cybersecurity Act transposing the NIS2 Directive (the Bill). Interested parties had the opportunity to send their opinions on the Bill during the one-month public consultation process.

The Bill was submitted to the Bulgarian parliament on 13 September 2024, and remains pending a vote. Considering the upcoming elections in Bulgaria, its adoption will be delayed.

The Bill envisages general risk management and reporting obligations for businesses, while detailed cybersecurity measures and obligations will be defined by ordinance within eight months of the amendments' enactment. The Bill also provides that a methodology for determining the significant and important entities shall be adopted within three months.

One of the main amendments proposed in the Bill is the extension of the scope of obliged entities. The following areas fall within its scope:

### **Annex 1 to the Bill**

- Energy (electricity, district heating and cooling, oil, natural gas and hydrogen);
- Transport (air, rail, water and road);
- Banking;
- Infrastructure on the financial market;
- Healthcare;
- Water for drinking;
- Wastewater;

- Digital Infrastructure;
- ICT Service Management (business-to-business); and
- Space.

### **Annex 2 to the Bill**

- Postal and courier services;
- Waste management;
- Manufacture, preparation and distribution of chemicals;
- Food production, processing and distribution;
- Manufacture of medical and in vitro diagnostic devices; computers, electronic and optical products; electrical equipment; machinery and equipment not classified anywhere else; motor vehicles trailers and semi-trailers; other transport equipment;
- Digital service providers; and
- Scientific research.

For significant and important entities as defined by the Bill, it introduces cybersecurity risk management measures and reporting obligations including, among others, to notify the Sector Computer Security Incident Response Teams (SCSIRT) of any significant incident within 24-72 hours.



The Bill envisages significant administrative fines for violations of the requirements:

- For significant entities, fines range from BGN 50,000 (approx. €25,565) to 2% of the total global annual turnover of the parent enterprise for the previous financial year. The minimum fine is BGN 20 million (approx. €10,225,838);
- For important entities, fines range from BGN 25,000 (approx. €12,782) to 1.4% of the total global annual turnover of the parent enterprise for the previous financial year. The minimum fine is BGN 14 million (approx. €7,158,086).



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

## **Concept for the development of artificial intelligence in Bulgaria until 2030**

Currently, the [Concept for the development of artificial intelligence in Bulgaria until 2030](#) adopted on 16 December 2020 by the Bulgarian Council of Ministers remains the main official public document in the field of AI. 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.

## **Information material issues by the Bulgarian Commission for Personal Data Protection for data subjects regarding Meta's intention to use photos and posts of its social network users to train its artificial intelligence**

In mid-2024, Meta Platforms Ireland Limited (Meta) announced that it plans to start using the publications, photos and their description, as well as the comments published on social networks Facebook and Instagram, to develop, train and improve Meta's service for artificial intelligence. Following this announcement, the Bulgarian Commission for Personal Data Protection (CPDP) published an [information material for the users of the social networks Facebook and Instagram](#).

Within the information material, the CPDP explained to users what Meta's AI training involves and that the extent to which Meta AI development will utilize posts and images restricted to users' friends remains unclear.

The CPDP informed the users of these social networks that access to information from Meta is difficult not only for the supervisory authorities, but also for the users.

The CPDP further explained that if users do not want their posts, images and comments to be used to develop and train Meta's artificial intelligence, they can object through the Objection Form available on the respective Facebook or Instagram pages.

The CPDP also informed that a mandatory field had been introduced in the Objection Form, which requires users to state the reason why they object to the planned processing. The required field was entitled "Please say how this processing affects you". The CPDP suggested that the reason a user gives could be, for example, that the user is worried, uncomfortable or they want to have control over their content. The CPDP emphasized that it is not necessary to write long sentences with official language and terminology, and that a user can also submit their objection in Bulgarian. After submitting the objection, the user will receive a confirmation code on the email with which the account was registered, which they should provide in the relevant objection form.

The CPDP explained that they tested the two forms and found that they were working and did not create obstacles with respect to the objection made. The result of the objection was visualized as a notification in the account (almost immediately after it was made) as well as in the email with which the account was registered and indicated in the objection. According to the CPDP, this suggested that Meta had a low threshold for accepting objections.

The CPDP also mentioned that users should note that the objection only applies to content that users have posted themselves. It does not apply if someone else's posts, photos or comments that contain user's personal data.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Data protection

### Finalization of the national legal framework in the area of accreditation

In its [Annual Reports for 2022 and 2023](#) the Commission for Personal Data Protection (CPDP) outlined its objectives and priorities, 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 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.

### Strategy of the CPDP for development in the fields of protection of the personal data and the protection of the persons who report or publicly disclose Information on breaches (horizon 2024-2029)

The strategy of the CPDP for development in the field of personal data protection setting strategic goals for the period 2017-2022 has already expired. The CPDP should finalize the activity of reviewing its strategic goals, which began in 2022. The new CPDP strategy should identify the priorities for development in the two areas of competence: the protection of personal data and the protection of whistleblowers.

## Cybersecurity

### Transposition of the NIS2 Directive

Bulgaria did not manage to transpose the NIS2 Directive into national law by the deadline of 17 October 2024. Considering the parliamentary elections, the adoption of the bill for amendment to the Cybersecurity Act is expected to happen no earlier than the end of 2024/beginning of 2025.

### National Cybersecurity Strategy

The National Cybersecurity Strategy of Bulgaria expired in December 2023, and adoption of a new one will require a decision by the Council of Ministers. It shall cover, among others: goals, principles and priorities; increasing awareness, knowledge and competences; stimulating research and innovation in the field of cybersecurity; cyber diplomacy; etc.

## Artificial intelligence

Following the entry into force of the Artificial Intelligence Act, Bulgaria as an EU member state has until 2 August 2025 to designate a national competent authority to oversee the application of rules on AI systems and carry out market surveillance activities.

# Cameroon

## Contacts



**Sandrine Soppo Priso**

Partner, Deloitte Legal Cameroon  
[ssoppopriso@deloitte.com](mailto:ssoppopriso@deloitte.com)



**Paul Raoul Nhanag**

Senior Manager, Deloitte Legal Cameroon  
[pnhanag@deloitte.com](mailto:pnhanag@deloitte.com)

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

## **Constitution of the Republic of Cameroon**

In the preamble to the Constitution of the Republic of Cameroon (Law No. 96/6 of 18 January 1996 revising the Constitution of 2 June 1972, as amended and supplemented by Law No. 2008/001 of 14 April 2008), it is stated that:

- Freedom and security are guaranteed to every individual with due respect for the rights of others and the best interests of the state; and
- Privacy of all correspondence is inviolable; no interference may be allowed except as provided in a judicial decision.

## **Regulation No. 01/20/CEMAC/UMAC/COBAC on the protection of consumers of banking products and services in the CEMAC (3 July 2020)**

As a member of the CEMAC, Cameroon must comply with this regulation.

The regulation outlines obligations for reporting institutions regarding the confidentiality, security, and protection of personal data, including biometric data.).

The community legislator prohibits payment institutions from collecting, storing, processing or disseminating sensitive consumer data.

Payment institutions are required to:

- Ensure the integrity and confidentiality of information such as: personal data and financial information of consumers through adequate control and protection mechanisms; and
- Implement security measures for premises, information systems and databases to prevent files from being misrepresented, damaged or accessed by unauthorized third parties.



## Draft law on personal data protection in Cameroon

Cameroon is preparing a privacy bill according to the competent services of the Ministry of Posts and Telecommunications

The bill stipulates that the following activities are subject to its provisions:

- Any processing of personal data of an individual residing in Cameroon, carried out by a controller established in Cameroon;
- Any processing of personal data of an individual residing in Cameroon, carried out by a processor established or not in Cameroon, if the controller is established in Cameroon; and
- Any processing of personal data of an individual of Cameroonian nationality carried out in a place where Cameroonian law applies by virtue of international law.

The bill aims to protect all automated processing in whole or in part, as well as all non-automated processing of personal data contained or intended to be contained in a data file, regardless of the form, by a natural person; the state and decentralized authorities, legal persons governed by public or private law.

This draft law provides:

- **Principles of personal data processing:** Personal data that is processed must be fair, transparent, collected for explicit, determined and legitimate purposes, adequate, relevant, non-excessive, accurate and kept in a form that allows the data subject to be identified.

- **Data protection authority:** The draft law outlines the establishment of a national authority for the protection of personal data – the Data Protection Authority; which will be responsible for protecting the rights and freedoms of natural persons regarding the processing of their personal data.
- **Transfer of personal data:** Transfer of personal data to a foreign country or international organization is authorized provided that the controller or processor in that foreign country or international organization provides appropriate safeguards and ensures that the rights and remedies of the data subject are respected.



# ? What are the most relevant **cybersecurity updates?**

## **The newly enacted Law No. 2023/009 of 25 July 2023 to institute the charter on child online protection in Cameroon**

The law instituting the charter on child online protection in Cameroon was enacted by the President of the Republic on 25 July 2023. The recently adopted legislation sets out the principles governing all activities involving children in the cyberspace, the role and responsibilities of different stakeholders (public authorities and the private sector) and the sanction regime attached to any breach of the legal provisions. In particular:

- The second chapter of this legislation outlines the roles of both public authorities and the private sector in ensuring a safe online environment for children. Public authorities are tasked with developing an appropriate framework, while the private sector is obligated to contribute to its implementation.
- This legislation outlines both general and specific obligations for stakeholders regarding online child safety. Generally, internet providers, digital content providers, and social network platforms must suspend access to any user upon request by competent authorities if they are found to have published content that violates the dignity and integrity of children. Specifically, internet service providers are required to provide users with guidelines on best practices for online safety and information about activities that undermine the dignity and integrity of children, including potential consequences.
- Ultimately a penalty regime has been defined by this new legislation including administrative sanctions and criminal penalties.



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

## The legal framework of artificial intelligence in Cameroon

Currently, Cameroonian legislation does not specifically address AI.

## AI and media summit: UNESCO in partnership with AUB calls on African media to seize technological advances

In March 2024, Cameroon hosted an international [summit on the use and impact of artificial intelligence](#), organized by the African Broadcasting Union (ABU) and the United Nations Educational, Scientific and Cultural Organization (UNESCO). The summit's theme was "Artificial Intelligence (AI): the new frontiers of African media".

The main purpose of the summit was to address the fundamental concerns arising from the emergence of artificial intelligence within African media organizations.

Perspectives for AI in Cameroon: Cameroon is committed to harnessing the opportunities presented by AI while mitigating potential risks. Key prospects include:

- The continuation and strengthening of the measures in progress, for a rational use of emerging technologies in Cameroon;
- The forthcoming organization of national consultations on artificial intelligence in collaboration with UNESCO, and all stakeholders of the ecosystem; and
- Continued awareness campaigns on the ethical use of digital platforms.

## Cameroon hosts consultations on AI integration in Cameroon

Yaoundé hosted the National Consultations on Artificial Intelligence (Conia 2024) between 25-26 June 2024.

These consultations were carried under the theme "Government approaches for better adoption of artificial intelligence in Cameroon" and intended to generate discussions on the challenges, opportunities and issues surrounding the use of AI in various sectors.

The Minister of Post and Telecommunications stated that the government plans to create incubators to encourage AI-enabled start-ups. This initiative aims to stimulate innovation and position Cameroon as a continental leader in the technological field. Collaborations with advanced international institutions are being explored to integrate AI into higher education curricula, thus generating interest among the younger generation.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## The domestication of the African Union convention on cybersecurity and personal data protection

Cameroon has not yet ratified the [African Union convention on cybersecurity and personal data protection](#), signed by the country on 12 August 2021. This convention entered into force on 8 June 2023.

This convention needs the prior approval of the parliament before being ratified by the President of the Republic. The final ratification and subsequent implementation remains to be done. The African Union convention carries on:

- Electronic commerce: State parties are called to ensure that e-commerce activities are exercised freely in their territories except in gambling, legal representation and assistance activities and activities exercised by notaries or equivalent;
- Data protection: The AU Convention aims at protecting the collection, transmission, storage or use of personal data by natural person, the state, local communities, and public or private corporate bodies; and
- Cybersecurity: State parties undertake to develop, in collaboration with stakeholders, a national cybersecurity policy which recognizes the importance of critical information infrastructure.

## Amendments to current national cybersecurity law

A need to amend certain provisions of Law No. 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon has already been identified.

A draft law was recently presented by the Ministry of Post and Telecommunications at the National Assembly. This draft law aims at amending the current legal framework of cybersecurity in Cameroon as it aligns with the best international standards like the Convention on cybersecurity of the European Council, commonly known as the “Budapest Convention”, signed on 23 November 2001.

This [draft law](#), if adopted with its actual content, will apply on the various forms of cybercrimes such as breaches of information systems security, electronic fraud, attacks on critical infrastructure and/or national security, privacy breaches, the dissemination of illegal content on the internet, in particular child pornography, racist or xenophobic messages or those which are likely to harm human dignity.

As discussions are ongoing, specific information on the amendments is not yet available.



## **The Ministry of Post and Telecommunications recently made public the project of law on data protection in Cameroon**

The National Assembly is currently studying the draft law submitted by the Ministry of Post and Telecommunications carrying on data protection regulation in Cameroon.

This [draft bill](#) aims to address an essential part of the data protection issue, which is currently absent from the Cameroonian legislative body. To this end, it describes the principles for processing personal data, their modalities, the obligations of the controller and its processor as well as the rights of the person concerned. The final adoption of this draft law by the parliament.



# Chile

## Contacts



**Ruby Soteras**

Partner, Deloitte Legal Chile  
[rsoterasf@deloitte.com](mailto:rsoterasf@deloitte.com)



**Oliver Ortiz**

Manager, Deloitte Legal Chile  
[oortizq@deloitte.com](mailto:oortizq@deloitte.com)

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

## New law on personal data protection

On 26 August 2024, the Chilean congress approved a new law that introduces in-depth and structural changes to the current regulation on personal data protection (as per the Bulletin No. 11.144-07 of the House of Representatives of the Chilean Congress), raising its standards to international levels, similar to those of the GDPR, one of the foundations for drafting this new law. The bill is currently under constitutional control, pending its publishing and official enactment.

This new legislation, in summary, strengthens the rights of data holders, regulates the processing of personal data providing for special categories of personal data, creates a new control authority (i.e., the Personal Data Protection Agency), and establishes specific infringements, high sanctions and applicable liabilities.

Among other issues, this new law stipulates the following:

- It establishes a set of **guiding principles for the protection and processing of personal data**, and reinforces the rights of the data subject, which obliges organizations that process personal data to have a data governance system in place, and checkpoints for its review.
- **New categories of personal data** are established (geolocation data, biometric data, data of children and adolescents), which generates the obligation to keep an inventory of data, and its classification, in order to carry out the necessary legal safeguards.
- **Security obligations** are added to be complied with by those responsible for data banks, requiring them to raise their security levels to international levels, requiring the observance of technical and organizational measures, when necessary.

- It stipulates the specific **duty to inform the agency by the most expeditious means possible of breaches of security measures** that entail a reasonable risk to the rights and freedoms of data subjects and result in the destruction, leakage, loss or alteration of personal data undergoing processing or unauthorized communication or access to such data.
- The **obligation to conduct data privacy impact assessments or PIAs** will be triggered when dealing with personal data that may pose a high risk to data subjects.
- A **special regulation is incorporated for the international transfer of personal data**, which implies following a series of rules in the event of such transfer.
- It establishes a system that promotes and encourages compliance with the law through an **infringement prevention model**, and the role of the **Data Protection Officer (DPO)**, which will serve as a mitigating factor in the event of violations.

This new law on data protection establishes that the **Data Protection Agency may impose fines of up to US\$1,466,600 approx.**, as well as accessory sanctions, such as the partial or total suspension of data processing operations and activities carried out by the data controller for up to 30 days, a term that may be renewable (even indefinitely).

In addition, the sanctions established by the Data Protection Agency will be recorded in a public and electronic registry, as a measure of disclosure of the sanctioned entities.

**Effective date:** This new law will become effective on the first day of the 24th month following its publishing in the Official Gazette, providing then a period of adjustment for the entities under its scope, which may take place at some point between 2026-2027.

# ? What are the most relevant **cybersecurity updates**?

## **New law regarding the cybersecurity framework and critical infrastructure**

On 8 April 2024, this new law was published, which, in summary, regulates the principles applicable to cybersecurity, cybersecurity obligations, essential services and vital operators, created the National Cybersecurity Agency, and establishes offenses and its corresponding sanctions.

Among other issues, this new law on cybersecurity, stipulates the following:

- The institutionality, principles and regulations that shall govern the cybersecurity activities of the state administration bodies and the relationship between these and individuals.
- The minimum requirements for the prevention, control, resolution and response to cybersecurity incidents that take place.
- The attributions and obligations of both state bodies and private institutions that possess critical information infrastructure, establishing control mechanisms and a system of infractions and sanctions.
- One of its main innovations is the **creation of a new supervisory body**, the National Cybersecurity Agency (NCA), an entity in charge of advising the President of the Republic on the matter, as well as ensuring the protection, promotion and respect of the right to information security.
- The law **shall be applicable to public and private institutions that provide services qualified as essential, and to those that are qualified as “operators of vital importance”**.

- Such entities, both public and private, will have the **obligation to report to the National Computer Security Incident Response Team (CSIRT)** to be created for this purpose, regarding the occurrence of cyberattacks and cybersecurity incidents that may have significant effects, within three hours of becoming aware of the event.

**Effective date:** Finally, regarding the **full force and effect of the law**, it may not take place until 2025 or 2026, since the President of the Republic has a period lasting until April 2025 to issue one or more decrees which will establish the period of vacancy before the entry into force of the provisions of the Law, as well as the date of commencement of NCA's activities, among other relevant aspects.





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

## Draft law on artificial intelligence

This new bill of law, submitted by the President of Chile as of May 2024, is currently on its first stage of the legislation process (Bulletin No. 16.821-19 of the House of Representatives of the Chilean Congress), and in summary, provides for a general regulation of artificial intelligence systems, specifying to which operators they will be applicable. The bill sets forth the principles that will regulate artificial intelligence systems, classifying and regulating the same according to their risks, creating a new technical entity (i.e., the **Artificial Intelligence Technical Advisory Council**), and establishing that the control and supervision of the obligations imposed by this new law shall be in charge of the Personal Data Protection Agency (created by the recently approved Bill of Law on Personal Data Protection, as per the Bulletin No. 11.144-07, mentioned earlier).

Among other issues, this new law on artificial intelligence provides that:

- The critical relevance of keeping **confidentiality of the information and data obtained from artificial intelligence systems**.
- That the **new Protection of Personal Data Agency shall oversee the supervision and regulatory compliance of this law**, and that within the members of the council there must be a representative of the aforementioned agency, as well as a representative of the National Cybersecurity Agency (previously referred).
- That artificial intelligence systems must be developed and used in such a way as to **minimize foreseeable damages**, and with regards to the regulation of high-risk systems, there shall be a **duty to implement safeguards** with management systems that minimize such possibilities.

- That high-risk artificial intelligence systems must have an **adequate level of cybersecurity**.
- The **scope of application** of this regulation shall include suppliers, implementers, authorized representatives, importers and distributors of artificial intelligence systems, even when providers and implementers are domiciled overseas, provided that the output information generated by the AI system is used in Chile, as detailed in the referred bill of law.

**Effective date:** One year after this bill is finally published in the Official Gazette.





# What are the most relevant expected developments in **data protection AI**?

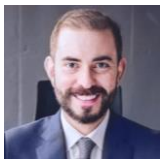
## Artificial intelligence bills

### Other bills on AI matters currently being discussed in the Chilean congress:

- Bill of law that establishes limits on the development of artificial intelligence, in safeguard of fundamental human rights (Bulletin No. 17.112-19 of the House of Representatives of the Chilean Congress).
- Bill of law that allows the use of artificial intelligence in the evaluation of mammography examinations (Bulletin 16.387-19 of the House of Representatives of the Chilean Congress).
- Bill of law that amends the Criminal Code regarding the crime of identity theft in the context of the use of artificial intelligence (Bulletin No. 16.112-07 of the House of Representatives of the Chilean Congress).
- Bill of law that amends the Criminal Code to incorporate, as an aggravating circumstance of liability, the use of artificial intelligence in the commission of a crime (Bulletin No. 16.021-07 of the House of Representatives of the Chilean Congress).
- Bill of law that amends the Criminal Code to punish the misuse of artificial intelligence (Bulletin No. 15.935-07 of the House of Representatives of the Chilean Congress).
- Bill of law that regulates artificial intelligence systems, robotics and related technologies, in their various fields of application (Bulletin No. 15.869-19 of the House of Representatives of the Chilean Congress).

# Colombia

## Contacts



**Jose Luis Jerez**

Partner, Deloitte Legal Colombia

[jjerez@deloitte.com](mailto:jjerez@deloitte.com)



**Lucía Tamayo**

Manager, Deloitte Legal Colombia

[lutamayo@deloitte.com](mailto:lutamayo@deloitte.com)

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

## **Record-breaking fine imposed on a telecommunications company**

**Resolution Number 35435** dated 27 June 2023, Superintendency of Industry and Commerce

On 27 June 2023, the Superintendency of Industry and Commerce, the authority on data protection in Colombia, imposed the highest fine to date for violations of personal data regulations in the country.

This sanction, amounting to US\$311,224, was imposed on a telecommunications company for the improper handling of data by obtaining referred phone numbers to offer telecommunications services through a commercial campaign.

The national authority emphasized that there is no other legal and constitutional interpretation different from the one that consent must be prior, explicit, and informed to be considered lawful. Otherwise, the right to informational self-determination, understood as the essential core of the right to habeas data, would be affected. In practice, this would mean that the data subject would lose control over their personal data.

## **Implementation of Law 2300 of 2023**

**Circular 001** dated 26 June 2024

Under Law 2300 of 2023, regulations were established to protect data subjects' right to privacy. This law defines the channels, times, and frequency for contact by entities overseen by the Financial Superintendency and other agents conducting collections, advertising, or commercial activities.

According to this law, unless the data subject requests to be contacted at different times, the contact conditions must be as follows:

- **Authorized channels:** Only those channels that have been previously, expressly, and informedly authorized by the data subject;
- **Contact hours:** Monday to Friday from 7 a.m. to 7 p.m., and Saturdays from 8 a.m. to 3 p.m. Contact is not permitted on Sundays or public holidays; and
- **Frequency:** Data subjects cannot be contacted by multiple collection agents through different channels within the same week or more than once in the same day unless the consumer requests it.

Additionally, External Circular 001 of 26 June 2024, from the Superintendency of Industry and Commerce, mandates that producers and suppliers of goods and services must consult the Excluded Numbers Registry (RNE) of the Communications Regulation Commission. This is to determine if the data subjects are registered and which channels are restricted, thereby avoiding sending advertising or commercial content to those who have opted out of such communications.

Authorizations for commercial projection purposes will be considered revoked once the data subject registers in the registry. However, if after this registration the data subject grants new authorization for advertising and/or commercial purposes, the data controller may contact them, always respecting the legal guidelines and conditions defined in the new authorization.

## Key aspects of requests for disclosure of workers' personal data

### [Ruling T-254 of 2024](#) by the Constitutional Court of Colombia

In the ruling T-254 of 2024, the Colombian Constitutional Court analyzed key aspects regarding requests for the disclosure of personal data of workers and determined that only information explicitly granted reserved status by the constitution and the law will be considered confidential.

For workers, the information that will be considered confidential includes data involving the rights to privacy and intimacy, such as details in resumes (CVs), employment history, pension files, and other personnel records held by public or private institutions, as well as medical histories.

The Constitutional Court established that data such as a person's name and national ID number are public data. Therefore, it is not possible to consider these as confidential or private data whose disclosure requires the authorization of the data subject.

In this regard, there is data that does not have a confidential nature simply because it is included in a worker's resume (CV). Only data considered sensitive due to its proximity to the data subject's privacy will be subject to confidentiality.

Consequently, all data contained in resumes (CVs) that are not sensitive will not be considered confidential. However, except for public data like name and national ID number, prior, express, and informed consent will be required to disclose them to third parties if requested through a right of petition, as these could be private or semi-private data.

## Instructions for corporate administrators on personal data processing

### [Circular 003](#) dated 22 August 2024

The Superintendence of Industry and Commerce, in its most recent Circular 003 of 22 August 2024, indicated that, as part of the duty of accountability, corporate administrators are required to adopt useful, timely, efficient, and demonstrable measures to ensure full compliance with the regulations regarding personal data protection within companies in Colombia.

Under this circular, corporate administrators will be jointly responsible for data processing when, together with the legal entity, they determine, regarding specific processing operations, the purposes or essential elements of the means that characterize the data controller over the database and/or its processing.

Some of the guidelines indicated by the Superintendence of Industry and Commerce are as follows:

- Administrators are obligated to comply with the regulations in this matter;
- They must have effective internal policies for data processing, which must be subject to constant monitoring and control;
- They must adopt internal mechanisms to enforce effective internal policies, including their implementation, training, and awareness programs;
- They must adopt preventive measures to protect the interests of personal data holders, such as privacy impact assessments; and
- They must establish guidelines to strengthen information security measures within the company.





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

## Processing of personal data in artificial intelligence systems

### Circular 002 of 2024 by Superintendence of Industry and Commerce

One of the biggest challenges generated by artificial intelligence is the protection and proper treatment of the personal data that is used to feed these systems. It is for this reason that it is possible to establish that the rules applicable in Colombian territory to the processing of personal data are also applicable in a general way when data is used in artificial intelligence systems.

In this way, for data controllers who also implement artificial intelligence systems, the duty to comply with the principle of demonstrated responsibility still stands, by virtue of which they must have the ability to prove that they have the technical and human measures in place to guarantee the quality, security and confidentiality of personal data.

Thus, despite the implementation of artificial intelligence systems, the owners of the information have the peace of mind that their data is still protected by the provisions of Law 1581 of 2012 and Law 1266 of 2008 and that non-compliance with these provisions will lead to sanctions imposed by the Surveillance Entity, which in the Colombian case is the Superintendence of Industry and Commerce.

## Standards applicable to public digital transformation

### Decree 1263 of 2022 of July 2022

This decree regulates the digital transformation of the public sector, within which it is possible to make use of artificial intelligence in order to improve the provision of state services in addition to implementing innovative tools that allow processes to be optimized in accordance with institutional needs.

All of the above, including the implementation of emerging technologies, must be done following the guidelines set for such purposes by the Ministry of Information and Communications Technologies, all of which are part of Digital Government policies.

Consequently, it is intended to achieve an automation of procedures within government institutions, this in order to make processes more efficient and to continue advancing in the implementation and digital transformation of the state.

# ? What are the most relevant **cybersecurity updates?**

## **General guidelines to strengthen digital security in Colombia**

### **Decree 338 of 2022 by the Ministry of Information Technologies**

Decree 338 of 2022 sets forth general guidelines to enhance the governance of digital security in Colombia. Its primary aim is to improve the management of digital security risks in essential services and critical cyber infrastructures of the country. This regulatory framework also seeks to increase trust and digital security, with the goal of maximizing socio-economic value generation through the Internet and cyberspace.

Also, the main modifications include: (i) the decree defines and classifies critical infrastructures and essential services necessary for the country; (ii) through the Colombian Cyber Emergency Response Team (COLCERT), the decree optimizes the attention to and response for digital security incidents; and (iii) clear policies and procedures for risk management and the protection of critical infrastructures are established.

The provisions of the decree apply to (i) entities that make up the public administration as defined in Article 39 of Law 489 of 1998; and (ii) private individuals performing public or administrative functions, referred to as "authorities" in the decree.

Additionally, the decree defines cyber defense as the state's ability to prevent and counteract cyberthreats or incidents that could affect society, national sovereignty, independence, territorial integrity, constitutional order, and national interests. This capability involves the use of military resources against cyber threats, attacks, or hostile acts.

## **Architecture, technology and security standards in open finance**

### **Circular 004 of 2024 by Financial Superintendence of Colombia**

This circular intended to provide instructions for the creation of some of the technological and security standards that financial institutions must implement in the case of open finance, also guaranteeing areas of transparency, security and efficiency in the processing of personal data.

This circular, in addition to requesting the creation of such standards, requires the modification of standards for access to information for financial consumers.

Additionally, it is established that financial institutions will have a period of 18 months for the implementation and adoption of architecture, technology and security standards with respect to open finance markets.



# What are the most relevant expected developments in **data protection, cybersecurity and AI?**

## **Artificial intelligence in the defense of labor rights**

### **Bill 130 of 2023** by Senate of the Republic of Colombia

The senate presented a bill that seeks to protect the rights of workers through the correct use and implementation of artificial intelligence tools, thus improving working life and productivity.

This regulation aims to protect the rights of workers in the face of the possible implementation of new technologies that can replace the work that people do for companies, so that humans continue to be an indispensable asset for industries and are not replaced in their entirety by artificial intelligence creations.

Therefore, instead of replacing the workforce, the optimization of existing processes, improvement of procedures and precision of results, among others, is sought.

Consequently, it is intended to make an analysis of jobs in which humans are better than artificial intelligence and the new technologies that have been developed to give priority to these, so that workers are protected against the decisions of companies to replace them. In addition to planning for the future in terms of the education of future generations and their preparation for the workplace.

## **Public policies for the implementation of artificial intelligence**

### **Bill 059 of 2023** by Senate of the Republic of Colombia

In the same sense as other regulations that are intended to be implemented in the field of artificial intelligence, this one aims to ensure that there is a prevalence of human intelligence over artificial intelligence, so that in terms of their application in various sectors of government, these new technologies are an element that works as a complement to the workforce and not as a replacement for it.

In environmental matters, it is intended that in cases of need and public interest, artificial intelligence can be used for the early detection of epidemics, the formulation of diagnoses and the development of medicines, among others.

Regarding personal data, there is still a duty to inform the owners when their data is used to feed artificial intelligence, as well as the result of such operations. Nor may artificial intelligence be used to engage in acts of unfair competition.

It is also proposed the creation of the Commission on Data Processing and Development with Artificial Intelligence to endorse new projects that involve the use of artificial intelligence, draft and disseminate technical regulations on the subject, advise congress on matters related to artificial intelligence and propose technological initiatives of artificial intelligence in public management, among others.

## Data protection and criminal law

### **Bill 050 of 2024** by the Senate of the Republic of Colombia

Victims of a crime face difficulties in providing material evidence such as images, audio recordings, video footage, and other data files containing detailed visual and/or auditory information about the reported incidents from the investigation stage of a criminal process. This issue stems from the inadequate exegetical interpretation of Laws 1266 of 2008 and 1581 of 2012 by those responsible for the handling of such data.

In this regard, Bill 050 of 2024 aims to amend Articles 137, 207, 213, and 244 of Law 906 of 2004, in order to ensure the proper involvement of victims within the criminal process during the investigation stage, by providing expedited access to various material evidence that demonstrates the commission of a typical conduct and that is stored as data in the form of images, audio recordings, video footage, among others. This data is handled by natural persons, legal entities, public, semi-public, private, or semi-private establishments that have recording or video surveillance systems. The aim is to prevent the rights of victims from being limited by arbitrary decisions and based on inadequate interpretations of the regulations on the protection and processing of personal data.

## Duty of information for responsible use of AI

### **Bill 091 of 2023** by Senate of the Republic of Colombia

This bill aims to guarantee the principles of safety, transparency, equality and equity in the responsible and ethical use of artificial intelligence. The foregoing, based on the basis that both natural and legal persons who make use of artificial intelligence must inform in a clear and accessible way that they have made use of it, which one they have used and what was the purpose of said use.

It is also intended that after the entry into force of the regulation, the state will prepare training sessions aimed at citizens through which they will prepare them for the use of artificial intelligence. One of the main objectives of the regulation is the responsible use of artificial intelligence within an ethical framework also guided by international standards applicable to the matter.

Finally, the law intends that research, development and innovation in the field of international intelligence in the public and private sectors be oriented within the framework of international cooperation to maintain the technical capacities of state entities in this regard.

Consequently, due to the rapid advancement of artificial intelligence, it is considered that early and anticipated preparation can help to better face the challenges and opportunities presented by this technological advance.



# Croatia

## Contacts



**Zrinka Vrtarić**

Director, Attorney-at-law, Deloitte Legal Croatia  
zvrtaric@kip-legal.hr



**Klara Jambrešić**

Manager, Attorney-at-law, Deloitte Legal Croatia  
kjambresic@kip-legal.hr

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

## **Regulation on the content and method of keeping records of employees employed by the employer**

The new Regulation on the content and method of keeping records of employees employed by the employer (Official Gazette No. 55/24, hereinafter: Regulation) came into force on 1 October 2024. The Ministry of Labour, Pension System, Family and Social Policy has issued a new Regulation to align the method of keeping employee records and their content with current laws, particularly the Labour Act, the Maternity and Parental Benefits Act, the Pension Insurance Act, and the Act on the Implementation of the General Data Protection Regulation.

The new Regulation has generally reduced the number of data points that employers are required to maintain in employee records. However, it introduces the requirement to record the date of submission registration (start, change, termination) for mandatory insurance registrations of employees as insured persons under an employment relationship, including voluntary pension insurance, if the employer contributes to it, as well as mandatory health insurance during work abroad.

According to the opinion of the Personal Data Protection Agency (AZOP), **employers are no longer required to and are prohibited from, storing employee records permanently**. Therefore, Article 9 of the new Regulation now precisely stipulates the retention periods and methods for storing employee data contained in documents, records, and files, depending on the type of data and document.

## **Key requirements for collecting copies of employee ID cards**

### **Opinion and guidelines of the Personal Data Protection Agency (AZOP)**

According to the new Regulation on the content and method of keeping records of employees employed by the employer (hereinafter: Regulation), employers are required to protect, store, and maintain, in original or copy form, the documents and records based on which they enter, modify, or delete employee data in their records. However, the Regulation does not explicitly require employers to collect or retain copies of employees' ID cards. The Personal Data Protection Agency (AZOP), **highlights that storing copies of ID cards is not a legal obligation under this regulation**.

In its opinion, AZOP pointed out that collecting and storing ID card copies involves a heightened risk of unauthorized or unlawful processing of personal data. For instance, ID card copies are often misused to enter into various contracts remotely. Employers are obliged to ensure appropriate security for personal data in line with the principles of integrity and confidentiality, as stated in the General Data Protection Regulation (GDPR).

If an employer decides to collect and store copies of employees' ID cards, they must have a legal basis for such processing according to Article 6 of the GDPR. Additionally, under Article 13 of the GDPR, the employer must inform the employee at the time of collection about the purpose and **legal basis for processing their data**. Employers should also adhere to the data minimization principle, ensuring that personal data is adequate, relevant, and limited to what is necessary for the intended purpose, removing or masking any irrelevant information on the ID card copy.

## Administrative fines for illegal processing of personal data through cookies

The Croatian Personal Data Protection Agency (AZOP) has recently imposed administrative fines on two gambling and betting companies due to illegal processing of personal data through cookies. The fines amounted to €20,000 and €30,000, following three violations of the General Data Protection Regulation (GDPR).

The violations included:

- Lack of legal basis: The companies collected and processed personal data from website visitors without a valid legal basis, violating Article 6(1) of the GDPR;
- Inadequate information provision: They failed to adequately inform users about data processing, violating Article 7 concerning the requirement for explicit consent for each type of cookie; and
- Transparency issues: The companies did not inform visitors about the processing of their personal data in accordance with Articles 13(1) and 13(2) of the GDPR, denying them critical information about the legal basis, functionality of each cookie, and storage duration.

In deciding on the fines, AZOP considered the nature, severity, and duration of the violations, as well as whether they were intentional or due to negligence.

## Guidelines for the use of smart cards with employee photographs

As of 28 June 2024, the Agency for Personal Data Protection in Croatia issued guidelines regarding the compliance of such smart cards with data protection regulations.

These guidelines emphasize the importance of adhering to the GDPR, specifically regarding the handling of personal and biometric data.

Under GDPR processing of biometric data (data derived from specific technical processing related to the physical or behavioral characteristics of an individual, enabling unique identification) is subject to strict regulations, highlighting the need for organizations to establish a lawful basis for their collection and use.

Organizations must ensure that personal data, including biometric data, is processed legally, fairly, and transparently, as mandated by Article 5 of the GDPR. This includes collecting data for specific, legitimate purposes and ensuring its accuracy and security. For instance, employers utilizing smart cards for access control must demonstrate that they have a valid legal basis for processing this data, as outlined in Article 6 of the GDPR. This could involve obtaining explicit consent from employees for the use of their photographs or biometric information for entry and timekeeping purposes.

The Croatian Personal Data Protection Act also specifies that biometric data can only be processed in the private sector if mandated by law or necessary for the protection of individuals and assets. Moreover, processing biometric data for timekeeping and access purposes is permissible only if employees have provided explicit consent. This requirement emphasizes the need for organizations to conduct thorough assessments of their data processing practices to ensure compliance with the law, particularly in handling sensitive biometric information.

As companies continue to implement smart cards for enhanced security and efficiency, they must navigate the complexities of data protection regulations to safeguard employee rights and maintain compliance. By doing so, organizations can effectively utilize smart card technology while fostering trust and transparency with their workforce.



# ? What are the most relevant **cybersecurity updates?**

## **New Cybersecurity Act**

### **Implementation of the NIS2 Directive**

The new Cybersecurity Act came into force on 15 February 2024, marking a significant update in Croatia's approach to cybersecurity. This legislation implements the Network and Information Security (NIS) 2 Directive of the European Union, which replaces the previous, more limited version of the law. The primary objective of the NIS2 Directive is to ensure a consistent level of cybersecurity across all EU member states, thereby enhancing the overall security posture of the Union.

One of the most notable changes introduced by the new law is the expansion of the number of entities covered under its regulations. The act now encompasses 19 sectors, categorizing them by risk level. This broadening of scope means that a wider range of businesses and organizations, including medium and large enterprises, utilities, logistics, pharmaceuticals, healthcare, and even educational and scientific institutions, will be subject to its provisions. Companies and organizations have a grace period of 18 months to align their operations with the new requirements.

Furthermore, the Cybersecurity Act establishes a framework for strategic planning and decision-making in the field of cybersecurity. It defines national frameworks for managing large-scale cyber incidents and crises, aiming to achieve and maintain a high common level of cybersecurity. This includes developing and continuously improving cybersecurity policies, enhancing public-private cooperation, promoting the integration of advanced technologies, and fostering education and training in the cybersecurity domain. By doing so, the act aims to bolster national resilience against cyberthreats, thereby ensuring the smooth functioning of critical societal and economic activities.

## **Implementing regulations**

The Cybersecurity Act mandates the adoption of several implementing regulations to enhance and clarify its enforcement.

- Within nine months from the act's effective date, the government is required to enact a regulation on the categorization of entities, the maintenance of a registry of key and essential entities, and the establishment of a special register for other relevant entities.
- Additionally, within 24 months, a medium-term strategic planning document will be issued to support the law's objectives.
- Within three months, the government is expected to adopt a national program for managing cyber crises, and within 12 months, a Cybersecurity Exercise Implementation Plan must be established.

These upcoming regulations will provide a crucial framework for effective application and further specify the Cybersecurity Act's execution requirements.





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

## Expected national AI development plan

The Republic of Croatia has not yet adopted a resolution on artificial intelligence or a national AI development plan, despite two proposals for such a resolution being submitted to the Croatian parliament by the opposition within the past year. The proposals called for a national AI strategy covering an initial phase up to 2030, followed by a long-term phase extending to 2050. In response, the Croatian government stated that establishing a national AI development strategy for 2030 and 2050 would not be optimal, as short- and medium-term plans and strategies would better address the rapidly emerging challenges of new technological trends and societal needs.

The Croatian government emphasizes that within the framework of the National Recovery and Resilience Plan 2021-2026, a reform measure, C1.1.2. R3 Establishing a Strategic and Operational Framework for the Digital Transformation of the Economy and Artificial Intelligence, has been proposed, along with the associated investment measure C1.1.2. R3-I1 Preparation of Strategic Documents for the Digital Transformation of the Economy and Artificial Intelligence.

The government also stated that the upcoming national AI development plan will define strategies for the increased application of artificial intelligence technologies to transform the Croatian economy. This plan aims to reassess business models and implement changes to boost productivity and create new areas of growth. In this context, the national AI development plan will provide a framework for the development of artificial intelligence, thereby contributing to its integration into both the economy and society.

Additionally, the Croatian government has indicated that it will, in due course, adopt a national framework for AI development, incorporating recommendations from the OECD Council on Artificial Intelligence. The provisions of the newly adopted Artificial Intelligence Act will be implemented at the national level, addressing key challenges highlighted in the proposed resolution.

Through these measures and activities, the government aim to establish a sound framework for the responsible integration of AI into the economy and society, while upholding European values and protecting citizens' fundamental rights.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Transparency Directive

### Implementation

In 2025, preparations will begin for the transposition of Directive (EU) 2023/970 of 10 May 2023 to strengthen the application of the principle of equal pay for equal work or work of equal value between men and women through pay transparency and enforcement mechanisms (Transparency Directive) into Croatian national law. While it is not yet certain that the legislative amendments will be enacted in 2025, work will commence toward implementing the directive. To incorporate its provisions, amendments to the Labour Act are anticipated, and certain aspects may require adjustments to the Gender Equality Act, the Public Procurement Act, the Civil Procedure Act, and the Anti-Discrimination Act to ensure comprehensive alignment.

## Cybersecurity

### Implementing regulations

In 2025, the following implementing regulations are expected to be enacted:

- A regulation regarding the categorization of entities, the maintenance of a registry of key and essential entities, and the creation of a special register for other relevant entities;
- A medium-term strategic planning document to support the law's objectives;
- A national program for managing cyber crises; and
- A cybersecurity exercise implementation plan to establish standards and procedures for conducting cybersecurity exercises.

## AI

### Development plan

The Croatian government has announced plans to introduce a national framework for the development of artificial intelligence in the near future. This framework will take into account the OECD Council's Recommendations on AI, aiming to establish a strategic approach for advancing AI in line with international standards.

# Cyprus

## Contacts



**Gaston Hadjianastassiou**

Partner, Hadjianastassiou, Ioannides LLC (member of the Deloitte Legal network)

[ghadjianastassiou@deloitte.com](mailto:ghadjianastassiou@deloitte.com)



**Christina Hadjivassiliou**

Senior Managing Associate, Hadjianastassiou, Ioannides LLC (member of the Deloitte Legal network)

[chadjivassiliou@deloitte.com](mailto:chadjivassiliou@deloitte.com)

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

## **Failure to respond to a DSAR leads to €2,000 fine**

In February 2024, the Office of the Commissioner for Data Protection of Cyprus (the Commissioner) imposed a fine of €2,000 for failure to comply with a data subject access request (DSAR).

Specifically, a complaint was filed against a company (the Controller) for failing to respond to a DSAR within the one-month legal time frame under GDPR Article 12(3).

The Commissioner contacted the Controller to investigate the case, and the latter admitted the delay, citing an internal error and high volume of requests, but eventually fulfilled the DSAR request. Despite mitigating factors, such as cooperation with the Commissioner and corrective measures, the Controller had two prior access request incidents, and the Commissioner imposed a fine of €2,000 for the violation.

## **Medical practitioner fined for GDPR data breach violations**

In December 2023, the Commissioner fined a medical practitioner who accessed sensitive medical information of an individual who was not her patient.

The main issues of the case included unauthorised access to sensitive personal data and improper processing. Specifically, when examining the facts of the case, the Commissioner took into consideration aggravating factors such as the sensitive nature of the accessed data and mitigating factors such as the lack of any previous infringements by the medical practitioner and eventually ruled that this was a breach of the principle of lawfulness, fairness, and transparency as outlined in Article 5(1)(a) of the GDPR, highlighting the importance of consent.

## **Data protection and privacy vs. freedom of expression**

A case arose involving the unauthorised disclosure of personal data by a publishing company through articles concerning the management of Turkish Cypriot properties.

In response to a parliamentary inquiry, the Ministry of Interior provided documents containing personal data of employees of the Turkish Cypriot Property Management Service and their family members. These individuals had submitted signed declarations with the understanding that their data would remain confidential. However, this information was later published in a national newspaper.

Following the lodging of complaints by affected individuals, an investigation determined that the publishing company violated the principle of proportionality under Article 5(1)(c) of GDPR, which mandates the minimization of data collection and processing. The company had failed to appropriately balance the right to freedom of expression with the right to privacy and data protection. As a result, an administrative fine of €5,000 was imposed, along with an order to delete the personal data from the newspaper's website. The company subsequently filed an appeal in February 2024, which is currently pending before the court.

This case emphasizes the importance of balancing freedom of the press with data protection rights, especially when personal data of a confidential nature is involved.





### Commissioner's Guidance on the operation of CCTV in private nursery schools (April 2024)

The Commissioner examined the legality of using CCTV systems in private nursery schools. While nursery schools are allowed to install CCTV in specific areas like points of entry and parking lots, they are prohibited from doing so in indoor spaces, classrooms, and playgrounds. Any form of surveillance that compromises privacy or monitors employee performance is not allowed.

The Commissioner noted that consent for such surveillance is considered invalid due to the unequal power dynamics between employers and employees and that audio recording is strictly forbidden.

### Commissioner's Guidance on the operation of CCTV in schools (April 2024)

The Ministry of Education, Sports, and Youth (MoESY) successfully completed consultations with the Commissioner regarding the installation of CCTV in schools to prevent and address violence and delinquency. Following a DPIA, key measures were proposed, including the installation of cameras at school entrances and perimeters, with recording strictly limited to school premises and operational only outside school hours. Footage will only be stored for 72 hours, with tightly controlled access, and warning signs will inform individuals of the CCTV presence. The Commissioner confirmed that the DPIA met the requirements of Article 35 of the GDPR and approved the CCTV installation in public schools.

MoESY will proceed with the implementation of these measures, starting with a pilot program in 10 schools.

### Commissioner's Guidance on the operation of CCTV in gyms (July 2024)

The Commissioner deemed that CCTV is permitted at gym entrances/exits, parking areas (if managed by the gym), the perimeter, and reception (focused on the cash register). However, it is not allowed in workout areas, kitchens, restrooms, changing rooms, or offices. Audio recording is strictly prohibited. Access to footage must be limited to authorised personnel within the gym and not via personal devices.

### Commissioner's Guidelines for sending promotional messages and making calls of a political nature

- **GDPR compliance:** Political communication, such as sending messages or making calls, must adhere to GDPR and national laws concerning direct marketing.
- **Personal data:** Information such as home addresses, email addresses, and phone numbers are considered personal data, and their use for political communication requires explicit consent from the individuals.
- **Electronic communication:** Sending messages via email, SMS, or automated calls requires prior consent. Consent must also be given for unsolicited calls or messages, with an opt-out option available in each communication.
- **Legitimate interest:** Political parties may rely on legitimate interest for communication with their members, but this must be balanced against the individual's right to privacy.
- **Consent requirements:** Consent must be specific, informed, freely given, and revocable at any time and obtained from the person directly.



## Cypriot university fined €45,000 following a cyberattack incident

In November 2023, a university in Cyprus was fined €45,000 by the Commissioner, following a cyberattack, which resulted in the unauthorized dissemination of, inter alia, student and graduate personal data.

The Commissioner found that the university had failed to implement sufficient security measures prior to the attack. The Commissioner also issued a mandate to the university requiring that a security officer be appointed to supervise the implementation of the improved security measures to be adopted by the university.

## Commissioner's GDPR Compliance Guide (February 2024)

The Commissioner issued a GDPR guide, providing a comprehensive framework for data controllers' and processors' compliance with the provisions of the GDPR.

The guide offers practical guidance to help organizations assess their current practices and identify areas for improvement concerning the following areas:

- The Data Protection Officer;
- Record of activities, impact assessment, and prior consultation;
- Data protection policy;
- Informing data subjects;
- Legal basis for processing;
- Exercising and fulfilling the rights of data subjects;

- Personal data breach;
- Direct marketing policy;
- Processing assignment contracts;
- Special processing activities;
- Transfer of personal data to third countries or international organizations;
- Information security policy;
- Organizational security measures;
- Technical security measures;
- Physical security measures; and
- Disaster recovery plan.

# ? What are the most relevant **cybersecurity updates?**

## **Appointment of the Digital Security Authority as the National Cybersecurity Certification Authority in Cyprus**

In January 2024, the Council of Ministers of Cyprus announced that the Digital Security Authority (DSA) was appointed as the National Cybersecurity Certification Authority (NCCA). The DSA is the competent supervisory authority responsible for the implementation of the NIS Directive 2016/1148 and NIS2 Directive 2022/2555.

- Its establishment and powers are in line with the provisions of the Cybersecurity Act (EU Regulation No 2019/881).
- The NCCA, as supervisory authority, will ensure that the rules included in the European cybersecurity certification schemes for ICT products, ICT services and ICT processes are applied. In particular, the NCCA will supervise the Conformity Assessment Bodies (CABs) and the relevant technical laboratories carrying out the technical assessments, which are involved in the certification processes. It will also handle any complaints related to Conformity Assessment Bodies and/or the certification of products and services.
- The ultimate goal of the NCCA is to contribute to making Cyprus a regional center for cybersecurity services, both through its responsibilities and its cooperation with other organizations.

## **Launch of the Cybersecurity Auditor Registry and the carrying out of cybersecurity maturity audits**

In September 2024, the Digital Security Authority (DSA) announced the launch of the Cybersecurity Auditor Registry (the Registry), established by Decision 245/2024 pursuant to the Security of Networks and Information Systems Law (89(1)(2020)), the national law implementing the NIS Directive (2016/1148), (the Decision). The Decision sets out the procedures and requirements for the carrying out of cybersecurity maturity audits on providers (as defined below).

- The Registry, which is publicly available, includes a list of the auditors eligible to conduct cybersecurity maturity audits on various entities including operators of essential services, providers of electronic communications networks and/or services and providers of digital services (the providers).
- Registered auditors will be conducting extraordinary or planned maturity audits in accordance with the yearly audit program of the DSA and as per the requirements of the Decision, the purposes of which include the determination of the level of maturity of providers and the setting up of an action plan by providers for the improvement of the level of security of their networks and information systems.
- Providers subject to maturity audits can choose between the registered auditors appearing on the Registry and will be required to enter into an agreement with their chosen auditor(s) that will govern their relationship for the purposes of the audit.



## **Issuance of a guide by the Digital Security Authority (DSA) on the NIS2 Directive**

The DSA, in the context of guiding the entities that will fall within the scope of the NIS2 Directive but also in the context of informing the public more broadly, has proceeded to create and issue a concise guide to the NIS2 Directive. This guide briefly covers the following:

- The sectors falling within the scope of the NIS2 Directive;
- The procedure for notifying security incidents;
- Cybersecurity risk management measures;
- Supervision of essential and important entities;
- The implementation of the NIS2 Directive and the relevant sanctions; and
- The responsibilities of entities' management bodies.





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

### **Deputy Ministry of Research, Innovation and Digital Policy collaborates with global AI leader**

In October 2024, the Deputy Ministry of Research, Innovation and Digital Policy signed a Memorandum of Understanding (MoU) with a leading commercial wholesale data center provider in the UAE which is part of an artificial intelligence and cloud computing global leader technology group.

The MoU serves as promising partnership that will position Cyprus as a major player in the global digital landscape and marks the beginning of a broader collaboration with the said global AI leader across a wide range of fields.

Working with the said global AI leader to integrate artificial intelligence, smart mobility and space technologies is expected to significantly enhance Cyprus' digital capabilities and further strengthen its position as a growing technology hub in the region.

### **Cyprus notifies the European Commission of the supervisory authorities supervising obligations under AI Act for protection of fundamental rights**

The Deputy Ministry of Research, Innovation and Digital Policy has notified the European Commission of a list of three national public authorities that will supervise or enforce compliance with the obligations under EU law to protect fundamental rights, in accordance with Article 77 of Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act). This action completes the first obligation of Cyprus for the national implementation of the AI regulation.

The list of public authorities of the Republic of Cyprus is as follows:

- Commissioner for Personal Data Protection;
- Commissioner for Administration and the Protection of Human Rights (Ombudsman); and
- Attorney-General of the Republic.

The authorities included in the list will be granted additional powers under the regulation to facilitate the exercise of their existing responsibilities to protect fundamental rights in cases where the use of artificial intelligence (AI) poses high risks to these rights. These powers will take effect from 2 August 2026.

The list will be reviewed whenever necessary to ensure that it remains up to date.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## **Amendment of the General Health System Law in line with data protection national law**

In February 2024, an amendment of the General Health System Law (89(I)/2001) (the Law) in line with the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data (Law 125(I)/2018) (the Draft Law) was proposed to allow the office of the Supervision Commissioner of the General Health System (the Office) to publish their reports on the Office's website and ensuring the protection of the personal data of the data subjects appearing on each report.

The Draft Law provides that the Office shall ensure that appropriate technical and organizational measures be taken by the Office including pseudonymization of personal data and the minimization of the personal data included in such reports. The Draft Law is now at the Standing Committee on Health for approval.

## **Amendment of the Forests Law in line with data protection national law**

In February 2024, the amendment of the Forests Law (25(I)/2012) (the Law) in line with the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data (Law 125(I)/2018) (the Draft Law) was proposed to enable the Director of the Forest Department, with the approval of the Minister of Agriculture, Rural Development and Environment, to install monitoring systems for fire prevention and environmental risk management purposes in forests.

The Draft Law is now at the Standing Committee on Internal Affairs for approval.

## **Amendment of national law implementing the NIS Directive in line with the NIS2 Directive**

In 2023, the Digital Security Authority (DSA), as the competent authority for the transposition of the NIS2 Directive, announced the opening of a public consultation on the amendment of the Security of Networks and Information Systems Law (89(1)(2020)), (the Law) (which is the national law implementing the NIS Directive 2016/1148 ) in line with the NIS2 Directive 2022/2555 (the Draft Law) and published the Draft Law on its website.

Among the amendments proposed in the Draft Law are the following:

- The drafting and implementation by the DSA of a national cybersecurity policy (Note: the last national cybersecurity policy prepared by the DSA was in 2021);
- The responsibility of the DSA on handling of large-scale cybersecurity attacks, which will be required to draft and implement a national response plan in relation to large-scale cybersecurity attacks; and
- Most importantly, various amendments were proposed in relation to security requirements, such as, the need to implement the appropriate operational and organizational measures to manage related risks, requirements on incident reporting and so on.

The public consultation has closed, but the Draft Law is yet to be passed into law. It seems that Cyprus may miss the transposition deadline set by the NIS2 Directive but is expected to proceed with the said amendments in the coming months.

## AI plans of the Deputy Ministry of Research, Innovation and Digital Policy

In May 2024, the Deputy Minister of Research, Innovation and Digital Policy of Cyprus mentioned in a conference that the Deputy Ministry has the following plans:

- The creation of a regulatory sandbox where companies can test AI systems in a controlled environment;
- The redrafting of the national AI strategy (Note: the latest national AI Strategy is from 2020); and
- The integration of AI in the public administration sector as well as other sectors of the economy including the private sector through specific use-cases. As a first step, the ministry will be introducing a digital AI assistant as part of its “Digital Citizen” initiative, the first iteration of which will be available on the new government portal by the end of 2024. The “Digital Citizen” initiative will be featuring an application through which official documents, such as driving licenses and biometric IDs, will be digitised and securely stored, gradually encompassing all government-issued documents.

In another conference in June 2024, the Deputy Minister of Research, Innovation and Digital Policy of Cyprus, mentioned of having plans of establishing a national AI Task Force. The AI Task Force will serve as a bridge between strategic policy and practical implementation, ensuring better governance and aiding in the alignment of AI projects with national goals.

In accordance with the Deputy Ministry of Research, Innovation and Digital Policy’s action plan published in June 2024, the Deputy Ministry of Research, Innovation and Digital Policy in collaboration with the national Social Insurance Services are planning to upgrade the national Social Security Information System (SISnet) which will include AI technologies.

# Czech Republic

## Contacts



**Jaroslava Kračúnová**

Partner, Deloitte Legal Czech Republic

[jkracunova@deloitteCE.com](mailto:jkracunova@deloitteCE.com)



**Edita Bolková**

Senior Associate, Deloitte Legal Czech Republic

[ebolkova@deloitteCE.com](mailto:ebolkova@deloitteCE.com)



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

## **Changes to “Data Box” legislation improves data protection for individuals**

The Czech Data Protection Authority (ÚOOÚ) has welcomed the amendment to Act No. 300/2008 Coll., on Electronic Acts and Authorized Conversion of Documents, which effectively reduces excessive intrusion into the privacy of individuals. The updated legislation modifies access to personal data of data box (Czech Data Box system is a secure electronic communication platform used for the exchange of official documents between public authorities and citizens or businesses) holders, specifically individuals and self-employed persons. Previously, a public register of data box holders required the mandatory listing of all holders, allowing personal details such as home addresses to be publicly accessible, which was deemed excessive and disproportionate. Following the DPA's intervention, the Digital and Information Agency promptly removed the lists of non-enterprise individuals from the open data system, which had enabled unrestricted access to personal data.

The revised law was published and has taken effect as of February 2024. The new legal framework replaces the automatic opt-out system with an opt-in model, meaning individuals will no longer be automatically listed; instead, they must actively request to be included in the register. This change not only enhances the protection of personal data but also grants self-employed individuals the right to request removal from the register, acknowledging their ability to change their minds after initially consenting to inclusion. Overall, these legislative updates represent a significant step toward strengthening data privacy rights in Czechia.

## **Transportation company fined for unsolicited commercial communications sent on behalf of a third party**

The Czech Data Protection Authority (ÚOOÚ) has imposed a substantial fine of nearly 8 million CZK (approx. €316,000) on a transportation company for sending unsolicited commercial communications on behalf of third parties without obtaining prior consent from recipients. Since 2015, the company has been disseminating promotional emails that featured offers for discounts and vouchers from third parties, violating Section 7 of the Czech Act on Certain Information Society Services.

The authority emphasized that the company was not permitted to invoke the so-called "customer exception" because it was not promoting its own products or services. The unlawful messages were inserted into purchase confirmation emails, leaving recipients with no option to refuse them. Additionally, the company failed to comply with other legal requirements, such as clear labeling of the communications and proper identification of the entity benefiting from these promotions. The penalty is among the highest ever levied by the ÚOOÚ, reflecting the extensive number of recipients – over 40 million – and the duration and manner of the unlawful communications.

## **Joint statement of Czech DPA and National Cyber and Information Security Agency warning users about mobile e-shop apps requesting unusual permissions**

The Czech Data Protection Authority (ÚOOÚ) and the National Cyber and Information Security Agency (NÚKIB) have issued a joint statement warning users about e-shop applications that request unusual permissions on devices and may collect excessive amounts of user data, including personal information. While various e-shop applications are currently available for download in the country, many ask for permissions that appear unnecessary for their primary function of buying and selling goods, such as access to location, contacts, and files. Operators of these applications may come from different regulatory environments, and their requirements could be inconsistent with Czech and European legislation, particularly concerning obligations to cooperate with state intelligence services of their country.

Users are advised to exercise caution when granting permissions to these applications and to review the information on personal data processing before agreeing to share data. They should look for specific details regarding the purposes of data processing, the extent of data collection, data retention periods, and the description of user rights. In light of the identified risks, including data collection that may exceed what is necessary for processing orders, users are urged to refrain from installing such applications on devices that handle sensitive information, like internet banking or government systems, and to uninstall them after one-time use if necessary.

## **Czech DPA imposes record penalty on a Cybersecurity Company for GDPR Violation**

Czech cybersecurity company was fined a record 351 million CZK (approximately €14 million) by the Office for Personal Data Protection for unlawfully processing personal data from users of its antivirus software and browser extensions which took place in 2019. The company transferred pseudonymized browsing histories of roughly 100 million users to its subsidiary, which provided marketers with detailed consumer behavior insights.

Despite the company's claims of robust anonymization, it was proven that the data could potentially be reidentified and linked with data subjects, compromising their privacy. The fine underscores the expectation that a leading cybersecurity firm should duly protect data and privacy of its users. The case was handled with other EU authorities due to its cross-border nature under the one stop shop mechanism.

# ? What are the most relevant **cybersecurity updates?**

## **Czech Republic Faces Delays in NIS2 Directive Implementation**

The European Parliament and the Council of the EU adopted the NIS2 Directive in December 2022 to enhance cybersecurity across the European Union. Member states are required to integrate these new regulations into their national laws by October 2024. Despite initiating the implementation process promptly, the Czech Republic is unlikely to meet this deadline. Initially, it was considered to amend the existing Cybersecurity Act No. 181/2024, but due to the extensive nature of the changes needed, a new Cybersecurity Act (Zákon o kybernetické bezpečnosti) will be introduced instead. The new law aims to expand the scope of regulated sectors and impose cybersecurity obligations on all medium and large enterprises in these sectors, potentially impacting 6,000 to 10,000 entities in the country.

The NIS2 Directive not only broadens the range of sectors covered but also sets more stringent security measures, including risk analysis, supply chain security, encryption, incident reporting, and employee training. This new directive introduces stringent penalties for non-compliance, with fines of up to €10 million or 2% of global annual turnover, alongside potential suspensions of cybersecurity certifications and bans on specific managerial roles. Despite the expected delay with implementation, organizations are encouraged to begin preparing for the new regulations as cybersecurity is increasingly critical irrespective of legislative obligations.

## **Czechia joins international initiative to define 6G network principles**

The Czech Republic, along with the United States, Australia, Canada, Finland, France, Japan, South Korea, Sweden, and the United Kingdom, has endorsed a joint statement on 6G networks. This statement outlines shared principles for the research and development of 6G communication systems, emphasizing collaboration in maintaining security, privacy, sustainability, and accessibility. Key aspects include ensuring the privacy of personal data, the trustworthiness of technology suppliers, and the resilience of network infrastructures. The collaboration will focus on adopting global technical standards, championing secure and resilient technologies, and fostering sustainable and affordable 6G deployments.

This joint initiative mirrors the collaborative efforts seen in the Prague Proposals for 5G security from 2019 initiated by National Cyber and Information Security Agency (NÚKIB) and aims to address the evolving complexities and risks associated with 6G network development. By aligning policies and setting the stage for globally interoperable and inclusive technologies, the statement calls for international cooperation to advance 6G networks that are protective of national security, environmentally sustainable, and accessible to all, including developing nations. The shared commitment is seen as vital for building a secure and inclusive digital future.

## **Czech Republic has published a national position on the application of public international law in cyberspace**

The Czech Republic has published a national position document on the application of international public law in cyberspace, created with the National Cyber and Information Security Agency (NÚKIB), the Ministry of Foreign Affairs, and the Ministry of Defense. This document addresses the challenges of rapid technological advancement and associated risks, detailing conditions for qualifying unlawful actions in cyberspace and permissible responses. It reaffirms that international law, including the UN Charter, applies to state behavior in cyberspace and is crucial for maintaining peace and stability. The Czech Republic seeks international consensus on this application and supports an international order based on law, enhancing participation in international cybersecurity law discussions, particularly within the UN's Open-Ended Working Group on cybersecurity (OEWG).

The position paper emphasizes the necessity of incorporating established international legal principles, such as sovereignty, prohibition of intervention, due diligence, and the peaceful settlement of disputes, into cyberspace. Developed with contributions from key national security agencies and approved by the Committee for the Foreign Security Policy Coordination, the document asserts that international humanitarian and human rights laws apply in the digital domain just as they do offline. It also discusses state responsibility, circumstances precluding wrongfulness, and neutrality within cyber operations, aiming to foster an open, secure, and peaceful ICT environment by advocating for responsible state behavior in cyberspace.

## **Czech Republic with its international partners has published joint recommendation document regarding security of software products**

The National Cyber and Information Security Agency (NÚKIB) of Czechia, in collaboration with various international bodies including the US Cybersecurity and Infrastructure Security Agency (CISA), FBI, NSA, and others, released a joint recommendation document titled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software." This document, aimed at technology manufacturers, emphasizes the importance of adopting Secure by Design and Secure by Default approaches. These methodologies focus on ensuring security at every stage of software development to produce more resilient products free of vulnerabilities. The updated recommendation, which builds on prior guidance issued by CISA in April 2023, incorporates feedback from numerous global stakeholders.

The emphasis on secure by design and secure by default is also a key component of the European Union's proposed Cyber Resilience Act, which seeks to mandate cybersecurity requirements for hardware and software products throughout their lifecycle. NÚKIB's involvement is part of a broader international effort to improve cybersecurity resilience and protect critical infrastructure and end-users. This initiative underscores the expanding global collaboration in cybersecurity, highlighted by interactions such as the Singapore International Cyber Week, where CISA's director urged broader community engagement in public consultation of the newly released document.





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

### **Czechia approves National Artificial Intelligence Strategy 2030**

The Czech government has approved the National Artificial Intelligence Strategy of the Czech Republic 2030 (NAIS), developed by the Ministry of Industry and Trade. This strategy aims to harness the potential of artificial intelligence (AI) to benefit the Czech economy and society, making the country not only a user but also a creator of advanced AI technologies. NAIS outlines priorities and goals up to 2030, with specific measures in seven interconnected areas: research and innovation, education and training, skills development and labor market impacts, ethical and legal aspects, security, industry and business, and public administration and services.

NAIS emphasizes the importance of strengthening AI research infrastructure, supporting top scientists, and fostering international collaboration to enhance the Czech Republic's competitiveness. The strategy also focuses on transforming the educational system to better prepare future AI professionals, promoting digital skills, and preventing digital exclusion. Legal and ethical frameworks are highlighted to build public trust and ensure responsible AI use. Security measures are planned to protect AI systems and data from cyberthreats, with active participation in international standards development.

In the business sector, NAIS aims to support AI startups, facilitate AI adoption in small and medium enterprises, and promote AI technology exports. For public administration, the strategy envisions improved efficiency and service quality through AI integration. An action plan will operationalize the strategy with initiatives like grant programs, business guides, and reskilling courses, supported by an investment of approximately 19 billion CZK. This plan will be regularly updated to adapt to evolving technological and societal needs.

### **Czech Republic proposes amendments to regulate AI-powered biometric identification systems**

The Czech Ministry of Interior has put forward significant amendments to the Police Act (No. 273/2008 Coll.) and the Personal Data Processing Act (No. 110/2019 Coll.) in anticipation of the EU AI Act. These proposed changes introduce a novel concept of an "isolated system" for remote biometric identification, subject to stringent regulations. The amendments aim to balance the potential benefits of AI-powered biometric identification with the need to protect individual rights and privacy.

The amendments newly define an "isolated system" as an AI system designed for urgent remote biometric identification of individuals in specific spaces. These systems are intended for use in areas where the presence of individuals is related to the specific purpose of the location.

The Office for Personal Data Protection (ÚOOÚ) has raised several concerns about the proposed amendments. There are fears that the amendments could lead to a "Chinese model" of widespread facial recognition camera systems and their extensive exploitation using AI. On top of that, the ÚOOÚ argues that the proposed regulations lack adequate controls, potentially leading to overuse of these systems and excessive interference with individual rights. The office opposes the potential interconnection of isolated systems, which could create a unified, comprehensive biometric identification network across diverse locations.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Artificial intelligence updates

The AI landscape in the Czech Republic will be shaped by the EU AI Act, which is expected to partially come into force in early 2025. This act will classify AI systems based on their risk levels, imposing strict requirements on high-risk systems, such as those used in critical infrastructure and safety applications. The Czech Republic will integrate these requirements into its national legal framework, which will involve setting up governance structures, such as a national competent authority and participation in the EU AI Board. Additionally, the Czech National Artificial Intelligence Strategy (NAIS) will continue to guide the country's AI development, emphasizing research, ethical considerations, and the integration of AI in various sectors. The strategy aims to align with the EU AI Act, ensuring that AI development in the Czech Republic is both innovative and compliant with EU standards. Overall, businesses and organizations in the Czech Republic should stay informed and prepare for these changes by assessing their current practices, investing in compliance measures, and seeking expert advice where necessary.

## Cybersecurity updates

The legal cybersecurity landscape in the Czech Republic will be heavily influenced by the transposition of the EU's NIS2 Directive, which must be implemented by October 2024, however, the transposition is facing delays, and the Directive is expected to be transposed in the last quarter of 2024 through the new Cybersecurity Act (Zákon o kybernetické bezpečnosti). This new legislation will expand the scope of existing regulations to include more sectors and significantly increase the number of entities classified as regulated service providers, estimated to rise significantly. Key obligations for these entities will include registering with the National Cyber and Information Security Authority (NÚKIB), implementing comprehensive security measures, and regularly reporting cybersecurity incidents.

## Data protection updates

### Czech DPA expected to join the fourth Coordinated Enforcement Action

In 2025, the Czech Republic is expected to participate in a significant Data Protection initiative initiated by the European Data Protection Board (EDPB). The fourth Coordinated Enforcement Action (CEF), set for launch in the first semester of 2025, will focus on the implementation of the right to erasure (the 'right to be forgotten') under Article 17 of the GDPR. Data Protection Authorities (DPAs) from various countries, including the Czech Republic, will join this action voluntarily to evaluate and compare how controllers implement this right. The goal is to identify both compliance issues and best practices, with an ultimate aim to enhance data protection measures across the EU. This initiative underscores the ongoing commitment to streamlined enforcement and cooperation among DPAs as outlined in the EDPB's 2024-2027 Strategy.

### Possible changes to Identity Card Act in the future

The Office for Personal Data Protection (ÚOOÚ) in the Czech Republic has expressed disagreement with a proposed amendment to the Identity Card Act that would allow for the indefinite inclusion of personal identification numbers (rodné číslo) on identity cards. The Czech parliament approved a bill that would rescind the current provision set to end the practice of recording these numbers on ID cards from 2025. From ÚOOÚ's perspective, this represents a departure from the trend since 2009 towards phasing out the use of personal identification numbers. The office argues that including these numbers on ID cards poses significant risks to personal data protection and privacy, especially given the ease with which ID cards can be copied, photographed, or scanned. The widespread availability of this sensitive information could lead to data linking and potential misuse in the virtual space, where control and rectification are challenging. ÚOOÚ emphasizes that removing the number from ID cards doesn't mean abolishing it entirely, but rather significantly limiting its potential for misuse. As ÚOOÚ disagrees with the amendment, the issue could be reopened in the future.

# Denmark

## Contacts



**Jeanette Vallat**

Partner, Deloitte Legal Denmark  
[jvallat@deloitte.dk](mailto:jvallat@deloitte.dk)



**Simone Mai Petersen**

Manager, Deloitte Legal Denmark  
[smpetersen@deloitte.dk](mailto:smpetersen@deloitte.dk)



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

**[Decision](#) from the Danish Data Protection Authority (in Danish: Datatilsynet) resulting in serious criticism, injunction and warning concerning Deposit Return System's (Dansk Retursystem) development of an app**

**Development of an app for deposit purposes, however, the app entailed processing of information concerning the user's accounts, balance and bank loans**

The component provided by the third party (provider) enables collection of, inter alia, the user's balances, identification information and transaction history and not only information relating to the user's account for purposes of paying the user for the deposit. Although such information were not shared with the Deposit Return System, it is against the GDPR to collect more information than what is necessary to fulfil the relevant purpose(s).

Prior to developing and implementing an app, the app must be subject to review, specifically the related processing activities relating to the app's design, including which personal data is collected and processed. The app's design must adhere to the GDPR regardless of how familiar or usual the components, which the app is based on, are.

The decision is of relevance for other actors, e.g., private undertakings and public authorities who have or is considering developing an app. With this decision, it is clearly established that the data controller is ultimately responsible for ensuring compliance with data protection principles (specifically principle of lawfulness, fairness, transparency and data minimization as well as privacy by design), also when relying on a third party for providing certain components of the app.

**Updated guidelines from the Danish Data Protection Authority (Datatilsynet) concerning handling of data breaches**

The [guidelines have been updated](#) to include more practical examples. Additional updates of the guidelines are expected throughout fall and winter 2024.



## Common principles on data protection of children and online gaming adopted by Nordic data protection authorities

### Guidance for compliant processing of personal data in the context of children and online gaming

The [principles](#) are based on four of the data processing principles set out under the GDPR:

- Fairness;
- Transparency;
- Data minimization; and
- Accountability.

Specifically, each of the four principles are reviewed and considered in relation to questions, points and considerations that can help data controllers to promote the principle in question in their processing activities and thereby, controllers can develop processing activities in a way that helps to protect the children's personal data.

The principles were adopted at the Nordic Data Protection Meeting in Oslo 30 May 2024.

## Updated guidelines from the Danish Data Protection Authority (Datatilsynet) concerning notification of data subjects

### A number of inspections performed by the Danish Data Protection Authority gave rise to updated guidelines

The inspections revealed that many organizations struggle to provide complete and understandable notifications to the involved data subjects. The [updated guidelines](#) address these shortcomings by detailing the necessary information that should be included, inter alia, the nature of the breach, the risks involved and protective measures and actions. The goal is to clarify legal requirements and improve transparency.

## **Updated guidelines from the Danish Data Protection Authority (Datatilsynet) concerning transfer of data to third countries**

**This updates reflect changes, including guidance from the European Data Protection Board (EDPB) and the EU Commission's adoption of an adequacy decision regarding the United States.**

The [updated guidelines](#) aim to help organizations navigate the evolving landscape of international data transfers and ensure compliance with GDPR when transferring data outside the EU. The guidelines are based on numerous examples on situations where personal data is transferred outside of the EU, inter alia, by way of a cloud solution, outsourcing of IT support and use of consultancy services. The key updates include adjustments to reflect the adequacy decision regarding the United States and incorporate EDPB guidance, emphasizing the need for thorough risk assessments and appropriate security measures. The updates help clarify compliance with GDPR in light of evolving international data transfer mechanisms.

## **Revised practice concerning recording of phone calls**

### **Adjustments to reflect changes within Europe**

The change allows recordings for training purposes without requiring explicit consent, provided the data subjects are informed and given the option to opt-out. The [revised guidelines](#) address practical challenges companies face in training staff while still maintaining respect for individual's rights. The aim is to provide more flexibility in call handling as long as transparency and choice are upheld for the data subject, e.g., a customer. In other words, the revision seeks to balance practical needs with privacy considerations.

# ? What are the most relevant **cybersecurity updates?**

## **The status on implementing the Network and Information Security Directive 2 (NIS2) in Denmark**

**NIS2** is aimed at enhancing cyber security across critical sectors, including energy, health, finance and digital services. It replaces the original NIS directive with stricter requirements for risk management, incident reporting and cooperation between EU countries. Denmark will not be able to comply with the deadline for transposing the measures into local law.

The Ministry of Defense (forsvarsministeriet) will present the primary legislation which will be the framework for implementing the measures of NIS2 across sectors. The primary legislation will authorize the relevant ministers (responsible for the involved sectors) to be specific on the NIS2 measures by way of executive orders (bekendtgørelser).

The energy sector, finance sector and telecom sector will not be comprised by the primary legislation as the implementation of the NIS2 directive will take place individually for each of these sectors.

The Ministry of Defense is responsible for coordinating the implementation of the NIS2 directive. In practice, the Cyber Security Center (CFCS) will coordinate the work med drafting the sector-specific executive orders. CFCS will draft a template executive order and, on this basis, start a dialogue with the competent authorities concerning the sector-specific executive orders. The executive orders will be negotiated with CFCS prior to being issued by the responsible minister.

On 5 July 2024, the Ministry of Defense presented a bill for consultation. It is proposed that the act will become effective on 1 March 2025. In conclusion, Denmark will be not be able to comply with the deadline on 17 October 2024.



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

## The Artificial Intelligence Act (the AI Act)

### Adoption of the AI Act in the European Parliament

The purpose of this regulation is to regulate the development and use of AI to ensure the protection of citizens' rights, safety and privacy while also promoting innovation. The act is the first global attempt to regulate AI technologies and is a key part of the broader digital transformation strategy of the EU.

On a national level, it is up to the assigned authorities to surveille and control the national market to ensure compliance with the AI Act. In Denmark, it is the Agency for Digital Government (Digitaliseringsstyrelsen) which is responsible for enforcing the AI Act. As part of the Danish government's digitalization strategy, the Agency for Digital Government and the Danish Data Protection Authority establish a so-called regulatory sandbox for AI, where private undertakings and public authorities can get access to relevant guidance and expertise concerning AI Act and GDPR when developing and applying AI solutions.

## Two projects elected for first round of the regulatory sandbox for AI

Upon reviewing 23 applications, [two AI projects have been elected for a development course in the sandbox](#)

The elected projects involve Tryg Insurance and Systematic (together with a number of municipalities).

The basis for electing these two projects has been to get the most use out of achieved knowledge for other actors and for society in general.

- **Tryg Insurance:** This project aims to develop an AI assistant which can assist with structuring and making summaries for insurance-related damage information, medical journals and other relevant documents relevant for processing a case concerning accident damages. Long-term, this system can be applied for developing a predictive model that can determine the degree of invalidity faster than currently.
- **Systematic (together with a number of municipalities):** This project is a public-private innovative cooperation between the municipalities of Copenhagen, Aarhus and Aalborg as well as Systematic. The project is named "Talt". The purpose of the project is to develop an AI solution which can reduce the documentation burden for staff within the health and care sector by enabling the staff to orally record documentation in journals.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Data protection

### Updated guidelines on risk assessments

The Danish Data Protection Authority (Datatilsynet) is expected to release updated guidelines on conducting personal data risk assessments.

## Cybersecurity

### Transposing the NIS2 directive to Danish law

The measures of the NIS2 directive will be transposed into Danish law by way of a primary legislation ([draft bill](#)) and sector-specific executive orders. It is proposed that the directive is transposed by way of minimum implementation.

## Artificial Intelligence

### Results from the sandbox projects

The Agency for Digital Government and the Danish Data Protection Authority have established a so-called regulatory sandbox for AI, where private undertakings and public authorities can get access to relevant guidance and expertise concerning AI Act and GDPR when developing and applying AI solutions.

The take-aways and results concerning the sandbox projects will be shared and made public on an ongoing basis. Finally, a final report summarizing the completed projects will be made public for others to benefit from.

# Ecuador

## Contacts



**Manuel Cartagena**

Partner, Deloitte Legal Ecuador  
[mcartagena@deloitte.com](mailto:mcartagena@deloitte.com)



**Sara Arias**

Manager, Deloitte Legal Ecuador  
[sariasrosero@deloitte.com](mailto:sariasrosero@deloitte.com)

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

## **Personal Data Protection Law**

### **Issued in 2023 but not yet fully in force**

The Personal Data Protection Law aims to guarantee the privacy and security of the personal information of all Ecuadorians.

However, this law has yet to be fully enforceable due to a delay in issuing its regulations and appointing the corresponding authorities.

Under the law, the Superintendence of Data Protection is created as the entity in charge of supervising and sanctioning companies or public agencies that violate the rights of users.

The most relevant provisions are:

- The creation of the Superintendence of Data Protection;
- Clear legal definition of what is deemed personal data:
  - Biometric data: Unique personal data, related to the physical or physiological characteristics, or behaviors of individuals which allows or confirms the unique identification of a person, such as facial images or fingerprint data, among others.
  - Genetic data: Data related to the genetic characteristics inherited by an individual which provide unique information about their physiology or health.
  - Personal data: Identifies or makes identifiable an individual directly or indirectly.
  - Personal credit data: Data on the financial behavior of an individual by analyzing their financial capacity.

- Data related to ethnicity, gender identity, cultural identity, religion, ideology, political affiliation, judicial background, migratory status, sexual orientation, etc.
- Data related to individual's physical or mental health, including the provision of health care services, which could reveal information regarding health.
- Rights of digital environments to access, rectify, cancel or oppose use of an individual's personal data that is usually stored by banks and public entities; and
- Minor and serious sanctions for entities in charge of personal data if information is not used or stored correctly. Minor penalties range from 0.1% to 0.7% of the entity's revenue. Serious penalties range from 0.7% to 1% of the entity's revenue.

The terms of this law will not be applicable for:

- Individuals using such data in the performance of family or domestic activities;
- Anonymized data, provided it is not possible to identify its owner;
- Journalistic activities and other editorial content;
- Personal data whose processing is regulated by specialized laws of equal or higher hierarchy in the field of risk management due to natural disasters; security and defense of the state. In all such cases, compliance with international standards on human rights and the principles of this law is required, and, as a minimum, with the criteria of legality, proportionality and necessity;
- Data or databases established for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions, undertaken by the competent state bodies in compliance with their legal functions; and
- Data that identifies legal entities.

# ? What are the most relevant **cybersecurity updates?**

## **Ecuador signs the Budapest Convention on Cybercrime**

The Convention on Cybercrime or Budapest Convention is an international treaty that seeks to tackle cybercrime and Internet crime by harmonizing laws between nations, improving investigative techniques, and increasing cooperation among the 75 signatory nations

On 4 July 2024, the National Assembly approved Ecuador's acceptance of the treaty.

Benefits of being part of the treaty include:

- Exchange of information;
- Transfer of probatory material in cybercrime cases; and
- Possibility of extradition for cybercrime offenders, subject to the internal regulations of each country. In Ecuador's case, such are applicable if the offense is deemed to be a transnational organized crime.

The convention aims to create a common criminal policy and defines the offences to which is applicable. Namely:

- Unlawful access and interception;
- Attacks on data and system integrity;
- Computer forgery;
- Computer fraud;
- Intellectual property infringements; and
- Child pornography and related crimes.

## **National Cybersecurity Policy**

In June 2021, the Ministry of Telecommunications and the Information Society enacted the National Cybersecurity Policy. The objective of this policy is to build and strengthen national capabilities to ensure the exercise of the rights and freedoms of the population and the protection of the legal assets of the state in cyberspace. It also created the National Cybersecurity Committee, which comprises various strategic relevant ministries.

The document also establishes a series of specific objectives and lines of action:

- Promotes public-private collaboration at national level, fostering trust and generating common responses to the risks and threats of cyberspace;
- Enhances the capabilities of detection, forecasting, prevention and management of cyber incidents, as well as management of cybersecurity crises in a timely, effective, efficient and coordinated manner;
- Protects the state's critical digital infrastructure from threats and risks in cyberspace to ensure its proper functioning and the provision of essential services;
- Safeguards public security in cyberspace, preventing and contributing to the investigation of cybercrimes, for the normal development of public and private activities, and the exercise of the fundamental rights of citizens in an environment of trust;
- Strengthens Ecuadorian diplomacy in the field of cybersecurity through cooperation spaces, at regional and international levels, in line with the national interest and Ecuador's foreign policy; and
- Generates a culture of cybersecurity and promotes the responsible use of cyberspace in the country.



## National Cybersecurity Strategy

On 3 August 2023, the National Cybersecurity Committee issued the National Cybersecurity Strategy.

The National Cybersecurity Committee comprises the Ministries of National Defense, Government, Interior, Foreign Affairs and Human Mobility, the Strategic Intelligence Center, the General Secretariat of Public Administration, the Presidency of the Republic, and the Ministry of Telecommunications and the Information Society.

The strategy was developed with the technical advice of the Cybersecurity Program of the Inter-American Committee against Terrorism of the Organization of American States (CICTE/OAS) and the European Union's Cyber Resilience for Development Project (Cyber4Dev). In addition, more than 170 actors from the public, private and academic sectors contributed as well as cybersecurity experts, representatives of the National Committee and all state functions.

The strategy establishes short, medium and long-term objectives to be met by all public sector entities and suggests guidelines for compliance in private sector companies and academia.

The strategy establishes the following as its main pillars:

- Governance and national coordination;
- Cyber resilience;
- Prevention and combatting cybercrime;
- Cyber defense;
- Cybersecurity skills and capabilities; and
- International cooperation.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Implementation of the Superintendence of Data Protection

Under the Personal Data Protection Law, the Superintendence of Data Protection will be established as the governing state entity in charge of all data protection matters, its regulation, overseeing the activities of those entities that handle personal data and applying the corresponding sanctions if information is not used and/or stored correctly.

The first Superintendent in office has recently been appointed and is in the process of setting up the entity.

It is expected to be fully in place and operating by the second half of 2025.

## Law on the Regulation and Promotion of Artificial Intelligence in Ecuador

### Draft laws currently being analyzed by the National Assembly

The National Assembly is currently reviewing two draft laws that seek to regulate all activities related to the research, development, implementation, commercialization and use of artificial intelligence systems by public or private, national or foreign entities. Such would apply regardless of whether the activities are undertaken in Ecuadorian territory or if they legally impact individuals or entities domiciled in the country.

The controller will determine the purposes and conditions of the use of the artificial intelligence system while the processor is the entity or individual that, under the authority of the controller of artificial intelligence, processes personal data on behalf of the latter.

The drafts also focus on complementary areas such as personal data protection, transparency and access to public information, consumer protection, competition and administrative law.

They also stipulate that original literary and artistic creations generated with the assistance of AI systems, including a substantial human creative contribution, may be protected by copyright.

If any of the draft laws are approved, such would become the first regulations in Ecuador to govern AI.

# Finland

## Contacts



**Jean-Tibor IsoMauno**

Senior Consultant, Deloitte Legal Finland

[jean-tibor.isomauno@deloitte.fi](mailto:jean-tibor.isomauno@deloitte.fi)



**Toni Oras**

Senior Manager, Deloitte Legal Finland

[toni.oras@deloitte.fi](mailto:toni.oras@deloitte.fi)

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

## Ensuring compliance with the GDPR

According to the Finnish Data Protection Act initiated in response to the GDPR and effective from 1 January 2019, the data subject has had the right to refer a matter to the Finnish Data Protection Authority (DPA) if the data subject considers that the processing of personal data concerning them violates the relevant legislation.

Until now there has not been any legal remedies in case of inactivity by the DPA, which has led to an official notice from the European Commission (6 April 2022), in which it considered that the Finnish legislation does not in all respects follow the requirements set by Article 78(2) of the General Data Protection Regulation (EU) 2016/679 and Article 58(2) of the Directive (EU) 2016/680.

Starting 1 January 2024, the data subject has a new legal remedy at hand, the right of appeal if the DPA is inactive for three months.

The DPA must handle the request initiated by the data subject within three months of its initiation or, if the matter cannot be dealt with within this time frame, inform the data subject of an estimate on when the decision will be issued within this time. The inactivity of the DPA will otherwise be regarded as a decision about the inadmissibility of the matter, to which the data subject has the right to lodge an appeal with an administrative court. The appeal must be filed before the DPA has processed the case or has given an estimate of the time of issuing its decision.

## Ensuring a due process and preventing identity fraud

Starting 1 January 2024 new legislation aims to ensure a more effective use of the resources of the DPA and improve the right of the data subject to have the case processed without delay.

Each year the Finnish DPA handles around 12,000 cases, of which data security breaches represent around one half. Many cases are legally simple, have established case law but require an administrative decision (e.g., when issuing an order to inform the data subjects of a data security breach or processing a complaint by the data subject focusing on a denied request to make a change in the medical record regarding the doctor's diagnosis or a description).

Decision-making in these cases, which do not require presenting them to the DPA can from now on be delegated to the DPAs presenting officers, together with the investigative powers following Article 58 of the GDPR. A presenting officer may also substitute either of the two deputy DPAs forming together with the DPA the collegial body, which decides on administrative sanctions following Article 83 of the GDPR.

In addition, the Finnish Data protection Act has been amended to avoid its use for cybercrime. The problem with the personal identification code has become that, in addition to its purpose of use, the unambiguous identification of a person (e.g., in a customer register), it is in some situations used either alone or together with the person's name for establishing the identity of the person. Establishing the identity of the data subject will from now on need other additional information typical for the customer relationship at hand, not easily accessible to everyone, if not otherwise expressly regulated. The controller should evaluate the applicable additional information on a case-by-case basis, taking into account the risks related to the situation.



## Outdated DSAR practices and a possible new trend in DPA sanctions

The DPA published 19 legally binding decisions between 1 September 2023 and 1 September 2024, six of which resulted to a reprimand of infringement of the GDPR. In addition, the DPA published two decisions which resulted to an administrative sanction, one of which is legally binding.

Several cases concerned the right of access, which will also be the topic of the third coordinated enforcement action by the EDPB, which is now presided by the Finnish DPA Anu Talus.

In these cases, the DPA reminded that a requirement to come on site to make an access request or to deliver the request by post is not in line with the GDPR but instead, organizations must specifically facilitate the use of access rights.

One case involving a client of psychotherapeutic services who did not receive any response to several data subject access requests (DSAR) resulted to a minor administrative sanction (€1,600). Some experts have argued, that since this decision there would be an upward trend in the level of so called GDPR fines issued by the Finnish DPA.

In that case access requests were made both personally and through a third party. This case together with a subsequent one involving the Finnish tax administration revealed that DSAR practices are still being partly based on practices dating prior to the GDPR.

The DPA pointed out in subsequent guidance that the GDPR does not prevent the use of a representative and the formal requirements for making and submitting a data request, e.g., by requiring a handwritten signature or using of a specific form, are no longer valid. However, the DPA noted, organizations must also ensure data security and find a right balance between the ease and the safe exercise of the data subject rights.

## Identifying the data subject in a proper manner

During the past year, the topic of data security and of appropriate technical and organizational measures was present in many binding DPA decisions.

One decision involved an app, in which the login did not require any password, but the person's membership number, the first two letters of the first and last name, and the year of birth. The membership number consisted of the country part, the club part and a one-to-four-digit member number, e.g., fi-123-4321, of which the last four numbers made up the actual membership number. The DPA considered the login mechanism as being predictable and easily deciphered by using an enciphering machine and not preventing unauthorized access to the personal data of the system users. To quote the DPA, the app's password policy was “weak or non-existent”.

Another decision involved an automated SMS, which was used to send laboratory test results together with the patient's identification code. The DPA pointed out the vulnerabilities of such systems to data leakage and ordered to limit the use of personal data in such messaging.

The question of identifying the data subject in a sufficient manner, but not too cumbersome manner surfaced also in several other decisions by the DPA. The DPA pointed out that while the GDPR has no provisions on how the identity of the data subject must be verified, the means must however be such as to ensure the use of the data subject's rights is facilitated. These do not include e.g., requesting additional but irrelevant or unnecessary information which can itself lead to breaching the principle of data minimization.

## Administrative Court decisions on administrative sanctions

### First administrative sanction upheld by Supreme Administrative Court

In September 2023, the Finnish Supreme Administrative Court issued a decision on an administrative sanction of €100,000 imposed on the Finnish postal service provider Posti Oyj from spring of 2020. This was the first sanction decision by the Finnish DPAs collegial body ever treated within the Finnish Supreme Administrative Court.

The case concerned the insufficient information of those who filed a notice of moving. It was noteworthy that the Supreme Administrative Court confirmed in its decision that the administrative sanction can be imposed without the DPA having first to use other remedies within its powers, such as an order or a reprimand.

### DPA's duty to investigate upheld by the Supreme Administrative Court

In September 2023, the Supreme Administrative Court issued a decision on the DPA's primary responsibility to provide evidence and to conduct its investigation based on the presumption of innocence. It pointed out to the punitive nature of the administrative sanctions which implies the presumption of innocence and the right against self-incrimination of the party concerned.

In this case a complaint was made to the DPA together with screenshots of a formular allegedly used by company A in its personnel selection. The formular included questions on the applicant's diseases as well as pregnancy, hearing, family relationships, birth years of children, parish and military rank. The Supreme Administrative Court considered that since the defendant's denying of using the formular since the coming into force of the GDPR was not obviously unfounded, the DPA could not base its decision solely on the refuted allegations.

## Court of Appeal confirms the prescription period of a GDPR claim

The Court of Appeal upheld the ruling of the District Court stating that a claim for damages based on an alleged violation of the GDPR does not have any specific prescription or action periods that should be applied instead of the general prescription period applicable to a claim for damages. Therefore, the general prescription period of three years is to be applied in these claims.

The case involved a data subject who in 2018 claimed a data breach had taken place within a city. In a response to the data subject during the same year the city deemed the claim unfounded. After the regular prescription period of three years had passed, the data subject renewed their claim and challenged the city to the district court claiming for €20,000 damages due to anguish caused by the alleged breach.

The data subject's claim was based on an allegation that a city official had committed a criminal offence in public office by illegally transmitting the data subject's health data, to which the prescription period is set in the Criminal Code to five years and that the general prescription period of three years following the Damages Act would thus not apply. The data subject also argued that a lack of notifying about the alleged data security breach could not lead to the loss and expiration of the data subject's rights.

The Court of Appeal upheld the District Court's view that the claims arising from Article 82 of the GDPR follow the common prescription period set by the Damages Act and that hence the claim could be rejected as inadmissible.

# ? What are the most relevant **cybersecurity updates?**

## Transposition of the NIS2 and CER Directives in progress in Finland

The NIS2 Directive will be transposed into national law by a new Cybersecurity Act save for the operators in the public sector, for which the Directive will be transposed into the current Act on Information Management in Public Administration. This latter act already contains stipulations on cybersecurity, although the cybersecurity implications of the NIS2 Directive will concern a more limited group of public sector stakeholders. The NIS2 Directive and CER Directive which will both apply from October 2024 are interlinked by their scope of application: the amount of the stakeholders of the former, and of the so-called essential entities, depends on how many organizations will be identified as critical in the meaning of the CER Directive. This will depend on the outcomes of the transposition of the CER Directive into national law, which is expected in early 2025. Although no major differences are expected, some will remain due to the differences in scope and definitions of these directives.

The government proposal estimates the Cybersecurity Act would cover around 2,500-5,000 entities, of which between 250-500 are essential entities. Of these 10-20 % were already covered by the NIS1 Directive, the biggest difference being the financial sector which is to be covered in its entirety by the DORA (EU 2022/2254) and its corresponding directive and transposing national legislation. However there remains still significant uncertainty concerning the number of new organizations coming under the scope of the Cybersecurity Act, especially in the fields of energy, chemistry and manufacturing. Without these industries, the scope is estimated to include only approximately 1,700-2,200 entities.

In the public sector the NIS2 Directive is estimated to cover about 160 public administration organizations, which are mainly all essential entities. It should be noted that public sector stakeholders will be exempted from possible administrative sanctions, even when they operate in a critical sector covered by the Cybersecurity Act and are subject to supervision and reporting duties of the relevant special industry.

Although the transposition will to a large extent be done on a minimal basis, some national discretion will be deployed, exempting entities operating in the field of national security, public safety, defense or law enforcement. In addition, the supervisory authorities will maintain a risk-based approach in their supervision and focus primarily on key actors.

During the committee stage of the governmental proposal concerns have been raised on how to ensure a uniform adoption and guidance of the obligations arising from European and national legislation – given the variety of authorities and superposed mandates. As a solution the committee encouraged to examine the possibility to establish one single secure notification channel for all notifications which are to be done through a secure channel (Whistleblowing Directive, GDPR, AI act, NIS2 Directive).

The parliamentary proceedings recognized the possibility of reducing costs and administrative burden of a single channel compared to several parallel secure notification channels. This could also enhance the exchange of information between the authorities and ensure a better coordination between the supervising authorities. It can be said, that this approach would also be in line with the policy of the current government policy which is that, as a rule, authorities are not given new resources to comply with new tasks resulting from European legislation.

The Finnish National Cybersecurity Center, operating under the Finnish Transport and Communications Agency, will be the responsible authority under the new act, as it has been previously during the NIS1 directive. It will hence act as the coordinator between cyber crisis management authorities and be responsible for preparing the national cyber crisis management framework required by the Directive to manage large-scale cybersecurity anomalies and crises in cooperation with other authorities.

For the entities involved there is a plan to offer an e-form for notifications, similarly to NIS1.



## Financial sector's digital resilience regulatory framework almost set

The previously mentioned DORA will, as an EU regulation, become directly applicable in the member states to financial entities falling under the scope of the regulation from early 2025. The DORA regulation is more comprehensive than the NIS2 and CER directives are and regulates digital resilience in the financial sector in more detail.

The transposition of the corresponding Directive (EU) 2022/2556 is almost completed and the national laws are expected to be soon published. The national legislation will include stipulations on the competent national authority and its competences, administrative sanctions and the exchange of information and cooperation between the authorities.

The Finnish Financial Supervisory Authority is proposed to be designated as the competent authority referred to in the DORA Regulation. It will also assume the tasks of the competent authority referred to in the NIS2 Directive and the CER Directive, regarding the banking and financial market infrastructure.

The tasks of the Financial Supervisory Authority will include the promotion of cyber-safe operating methods to the financial market operators and of the capacity of critical financial market's critical players to tolerate digital disturbances.

During the parliamentary proceedings, securing the digital operations of the operators in the employment pension insurance sector, to which the DORA does not apply raised concern. What kind and how detailed legislation this will require will be assessed separately.





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

## **Finland pursues in regulating the national bodies and the sanctions**

An inter-ministerial working group was set in April 2024 regarding the supplementary provisions on the supervision of the AI act released a draft government proposal on the supervision of certain artificial intelligence systems and amending related laws in October 2024.

The final version of the government proposal is expected to be presented to the parliament in March 2025.

The proposition is that the market surveillance authorities referred to in the Annex I, section A of the AI act will be the ones that currently assume that role following the Union harmonization legislation and the national legislation which has been established when transposing it.

This mandate has been given to the Finnish Safety and Chemicals Agency (points 4,5,7,9, 10 and point 2 together with the Finnish customs of Annex I, section A), the Finnish Transport and Communications Agency (points 3, 6), occupational safety and health authorities, i.e., the Ministry of Social Affairs and Health and the work safety departments of the regional administrative agencies (points 1, 8, and partly 9), and the Finnish Medicines Agency.

The DPA is proposed to act as the surveillance authority of the prohibited AI practices.

The surveillance of high-risk AI systems referred to in Article 6(2) and listed in Annex III of the AI act is proposed to be shared among the DPA (points 1, 3, 4, 5 b, 6,7 and 8 of Annex III), as well as 7 other surveillance bodies. This would be in line with the EDPB opinion 3/2024 (point 9).

The surveillance of high-risk AI systems in the area of critical infrastructure is proposed to be done by the Finnish Transport and Communications Agency, the Energy Authority, the Finnish Safety and Chemicals Agency and the Centre for Economic Development, Transport and Environment of Southern Savonia.

The Financial Supervisory Authority and the National Supervisory Authority for Welfare and Health are proposed to share responsibility for the surveillance of high-risk AI systems in the area of access to and enjoyment of essential private services and essential public services and benefits (point 5).

The Finnish Transport and Communications Agency will act as the single point of contact. Its tasks would be the transmission of information and the fulfillment of the reporting obligations arising from the regulation as well as providing expert support to other market surveillance authorities. In addition, it is proposed to be designated as the surveillance body for the transparency obligations arising from article 50 (points 1,2 and 4).

The working group proposed the Finnish Safety and Chemicals Agency to act as the surveillance authority of last resort, meaning surveillance of such high-risk AI systems which does not fall within the mandate of the existing bodies. This raised the question of whether that would lead to acting as a second single point of contact, and thus it was not included in the final draft.

Concerning the notifying authorities the proposition is that they would be the same as the ones designated as the notifying authorities for the products referred to in the Union's harmonization legislation following Section A of Appendix I of the AI act (Ministry of Economic Affairs and Employment, the Finnish Transport and Communications Agency and the Finnish Medicines Agency together with the Ministry of Social Affairs and Health).

Concerning the administrative sanctions, these will be imposed by a collegial body if the sanction exceeds €300,000. For the sake of uniformity of practice, all punitive penalty payments would be concentrated in one body. The collegial body would also impose fines to notified bodies, regardless of their amount. In addition, similarly to the Data Protection Act, the administrative sanctions are proposed not to be set to public bodies.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Objective to enhance the flow of data and level the playing field

The current government has in its governmental plan from 20 June 2023 envisaged an overall reform of data protection legislation that will include abolishing laws and regulations that hinder the free movement of information, the appropriate use of cloud services, or otherwise the appropriate organization of public services. This will be done by using, if necessary, the national margin of maneuver of the GDPR to a greater extent.

This objective will probably be felt the most within the sector of social and healthcare services, where the current legislation regarding data management including advice, guidance and supervision are planned to be reformed. This will include developing the current norms on the processing of personal data, so that the data collected within the social and health services can be used more efficiently between different operators, both locally and nationally.

By streamlining the flow of information, the reform aims to promote the functionality of service chains and of the integrity of the services and to anticipate the customer's service needs.

The actors involved are the publicly funded social and healthcare services providers, the 21 newly established well-being counties as well as the municipalities in which services such as the promotion of well-being and from 2025 onwards employment services are offered.

A working group has also been established to make some adjustments in the legislation concerning the secondary use of social and healthcare data, which has been a model in the drafting of the act on European health data space, especially its secondary use parts.

The aim of the adjustments is to enable a more attractive operating environment for domestic and international operators in the fields of research and development and innovation industries and to promote the health and well-being sector. In parallel, there is a need to find out the possibilities of ensuring the preservation of pictorial material for longer time periods for their use in both primary and secondary purposes.

In connection with the overall reform, the imposition of administrative sanctions following the GDPR to both public and private sectors will be explored.

The governmental plan objectives have since been studied by a coordination group, of which an interim report was published for comments during June 2024.

The report states that only a small number of laws and regulations related to the processing of personal data significantly hinder the appropriate organization of the public services. Instead, several issues relating to the interpretation of either the GDPR, the Data Protection Act or sector-specific laws and regulations on the processing of personal data have been identified under several administrative branches and that these may impact the organization of public services.

In addition, some specific articles may require further guidance, e.g., the use of public interest as a legal basis when performing a public authority's planning and investigation task and in which situations the processing may be based on consent or on legitimate interest.

# France

## Contacts



**Tony Baudot**

Director, Deloitte Legal France  
[tbaudot@avocats.deloitte.fr](mailto:tbaudot@avocats.deloitte.fr)



**Morgane Bourmault**

Manager, Deloitte Legal France  
[mbourmault@avocats.deloitte.fr](mailto:mbourmault@avocats.deloitte.fr)



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

## Elections

**France held both European and legislative elections in 2024, the latter prompted by President Macron's dissolution of the National Assembly**

For the elections of the European Parliament, [the CNIL \(the French data protection authority\) has intensified its actions during the electoral period to promote voters' rights and ensure compliance with the GDPR in political communications](#). It sent letters to political parties and candidates to raise awareness about data protection and provide practical tools.

Simultaneously, the CNIL established **a platform for voters to report GDPR violations**, supplying information about their rights.

The CNIL prepared for the European elections by **alerting parties about the protection of personal data**, notably during an awareness session in March 2024.

During the campaign, the CNIL registered 167 reports and two complaints, in response to which it issued four legal reminders. A significant change was observed in the methods of solicitation: automated calls, which represented 93% of reports in 2019, have been replaced by SMS, accounting for 88% in 2024.

For the legislative elections of 2024, again [the CNIL played a major role in protecting the voters' data in different ways](#). It sent new letters to parties, encouraging them to respect the protection of voters' data and announcing formal checks in case of high complaints. It requested parties to designate a contact and answer questions regarding their political solicitation practices by 22 June 2024.

The reporting platform for voters introduced by the CNIL during this period also **provided voters with information about their rights and a form to report alleged violations of the GDPR**.

## Education – rights of minors

**In response to growing concerns about children's rights, the CNIL has updated and expanded its online resources for children, teenagers, and educators**

[Digital parenting is a priority for the CNIL](#). According to a 2023 study, 67% of children aged 8 to 10 use social media, but 70% of parents feel they lack control over their children's usage.

However, parents play a key role, particularly by giving consent for children under 13 to sign up for these services and guiding them in learning **best practices for protecting their privacy online**. Children's use of digital devices often causes tension within families, and parents are seeking practical advice.

The CNIL addressed this need by offering educational resources and taking actions in this field.

The CNIL also welcomes the Arcom's (French regulatory authority for audiovisual and digital communication) [new framework](#) for age verification systems, which includes many of its recommendations on data protection and privacy.

The framework requires an independent third-party verifier to handle age checks, separating the process from pornographic sites. It also mandates a "double anonymity" solution: sites verify users' age without knowing their identity, and the verifier doesn't know which sites are accessed.

The CNIL supports solutions where users can locally generate proof of age, reducing reliance on third parties. The CNIL stresses that age verification is just one tool to protect minors online, and its use should be limited to specific cases. Widespread implementation could infringe on individual rights, particularly freedom of expression.



## Health data: a reminder of security and confidentiality measures for access to computerized patient records

The computerized patient record (DPI – *Dossier patient informatisé*) centralizes all patient health data within a healthcare facility, facilitating easy access for healthcare professionals. Between 2020 and 2024, the CNIL conducted 13 inspections in response to reports of unauthorized access to patient data.

These inspections revealed that some facilities had inadequate security measures, allowing unauthorized access to medical data.

On 9 February 2024, [the CNIL published recommendations to health establishments](#) to remind them that due to the sensitivity and volume of the data it contains, the DPI requires enhanced security measures, mainly relating to authentication policy, authorization management and access tracking.

## Genetic tests on the internet: risks of data disclosure and reuse

[Websites offering genetic testing collect sensitive data, including ethnic origins and health predispositions, often without the relatives' consent](#). In France, genetic tests are restricted to judicial, medical, or research contexts, requiring individual consent, with significant penalties for unauthorized testing.

[The CNIL monitors these practices due to risks of data breaches and discrimination](#).

In this sector, companies provide limited assurances about data security, and vague terms regarding data sharing which the CNIL considers are raising concerns about misuse. Overall, the CNIL reminds that strict regulation and oversight in genetic testing are essential to protect personal privacy and sensitive information.

## Mobile applications: the CNIL publishes its recommendations to better protect privacy

On 24 September 2024, following a public consultation, [the CNIL has published the final version of its recommendations](#) to help professionals design mobile applications that respect privacy.

Starting in 2025, the CNIL will ensure that these recommendations are taken into account through specific control campaigns.

The CNIL's recommendation targets all players involved in developing and making available mobile applications, to ensure enhanced protection of personal data at every stage: mobile application publishers, mobile application developers, software development kit providers, operating system suppliers, and application store providers.

## Open data practices and reuse of personal data on the internet

[The CNIL addresses the rapid development of open data practices](#) while emphasizing privacy protection. In 2023, [a public consultation gathered 26 contributions from diverse stakeholders](#), leading to clarifications on data reuse practices.

The CNIL has created resources for [data publishers](#) and [reusers](#), helping them understand their legal obligations regarding data processing. The updated guidance published by the CNIL outlines the economic, scientific, and democratic importance of data sharing, alongside the risks it poses to individual rights.

The CNIL plans to continue enhancing these resources and exploring data-sharing scenarios under current French and European laws, ensuring innovation while safeguarding privacy rights.

## Recent cases

**27 December 2023:** The CNIL [fined Amazon France Logistique €32 million](#) for implementing an excessively intrusive employee monitoring system and for insufficiently secured video surveillance.

Amazon's large warehouses utilize scanners to track employee productivity in real-time, resulting in detailed data collection on individual performance, including "idle time" and scanning speed.

The CNIL deemed the monitoring practices excessive, as they created undue pressure on employees and violated GDPR principles, particularly regarding data minimization and lawful processing. Additionally, issues were identified concerning inadequate information provided to temporary staff and insufficient security measures for video surveillance systems.

**29 December 2023:** The CNIL [fined Yahoo EMEA Limited €10 million](#) for failing to respect users' cookie preferences on "Yahoo.com" and for not allowing "Yahoo! Mail" users to withdraw consent freely.

Following 27 complaints, the CNIL found that Yahoo deployed cookies without consent and discouraged users from retracting their consent by linking it to the access to services. The CNIL highlighted that such practices violate the principle of freely given consent under data protection laws.

**31 January 2024:** The [CNIL fined FORIOU €310,000](#) for using data supplied by data brokers for commercial canvassing purposes, without ensuring that the persons concerned had validly consented to being canvassed.

**4 April 2024:** The CNIL [fined HUBSIDE.STORE €525,000](#) for using data supplied by data brokers for commercial canvassing purposes, without ensuring that the persons concerned had validly consented to being canvassed.

**5 September 2024:** [CEGEDIM SANTÉ, a provider of management software to medical practices, was fined €800,000](#) by the CNIL for unauthorized processing of pseudonymous health data used in studies.

The company failed to secure the necessary CNIL authorization and processed data unlawfully by allowing automatic downloads of patient information.

The CNIL concluded that the risk of reidentification was significant due to the depth of data collected, prompting the penalty, although CEGEDIM is no longer responsible for such processing since July 2024.

**8 October 2024:** Since June 2024, [the CNIL has issued 11 new penalty decisions under its simplified procedure](#), for a cumulative fine amount of €129,000.

The main violations concern:

- Failure to comply with the principle of data minimization (video surveillance of employees and systematic and complete recording of telephone conversations);
- The lack of means to refuse cookies as easily as to accept them; and
- Failure to cooperate with the CNIL; failure to respect people's rights (failure to respond within the stipulated deadlines); failure to inform individuals (customers and employees).

# ? What are the most relevant **cybersecurity updates?**

## Cyber review of the Paris 2024 Olympic and Paralympic Games

The French national agency for the security of IT systems, *Agence nationale de la sécurité des systèmes d'information* (ANSSI), led the cybersecurity preparations for the Paris 2024 Olympic and Paralympic Games

Ahead of the Paris 2024 Olympic and Paralympic Games, [the ANSSI implemented a robust system to protect against cyberthreats](#).

This strategy focused on several key areas: understanding potential cyber risks, securing critical information systems, protecting sensitive data, raising awareness, and preparing for any cyberattacks.

With the support of the Ministry of the Interior and the Games' organizing committee, the ANSSI worked with nearly 500 entities to assist them in their cybersecurity preparation.

These organizations received **cybersecurity audits, technical support, and enhanced detection systems for early threat identification**. To raise awareness, the ANSSI launched campaigns, including seminars and email distributions, starting in 2023. The ANSSI also provided exercise kits to help organizations prepare independently.

Additionally, a **unique coordination framework** was established, involving both national and international stakeholders, to handle any reported cybersecurity events during the Games.

Between May and September 2024, the ANSSI handled 548 cybersecurity events, most of which were relatively minor, with no major disruptions to the Games. Although several incidents occurred, such as DDoS attacks and system compromises, none affected key ceremonies or the smooth running of the events.

## The SREN law, aimed at securing and regulating the digital space in France, came into force on 21 May 2024

Enhancing digital safety with measures like anti-scam filters, rapid blocking of child pornography, and social media bans for cyberstalkers, protecting users, especially youth and businesses

This law, inspired by European digital regulations and parliamentary reports, **mandates stricter age verification for pornographic sites** and penalizes non-compliance. The Arcom (French regulatory authority for audiovisual and digital communication) can block or delist violating sites. It also enforces swift removal of child pornography, mandates warnings for violent content, and grants actors' rights to remove unauthorized videos.

This law introduces **an anti-scam filter** to protect citizens from **fraudulent sites**, increases penalties for online hate and cyber harassment, and allows social media bans for offenders. It targets deepfakes and disinformation from sanctioned foreign media.

**Educational programs will address AI risks**, and the Arcom can order the shutdown of propaganda channels. A digital citizen reserve will also be created for awareness.

Also, this law reduces cloud dependency through data migration regulation and cloud interoperability requirements, enforces stricter tourist rental rules, and introduces a three-year experimental framework to regulate Jonum, a hybrid online game, addressing addiction and money laundering concerns.

Finally, this law aligns French legislation with the DSA (Digital Services Act) and DMA (Digital Markets Act), giving the Arcom, DGCCRF (the French directorate for consumer affairs and fraud control), and CNIL **new responsibilities for regulating digital services and marketplaces**. It also establishes a national coordination network for digital regulation, involving administrative authorities and state services to enhance cooperation.

## Recommendations for hosting sensitive information in the cloud

### The ANSSI's cloud hosting recommendations help entities choose appropriate cloud solutions aligning with the state's "cloud-first" doctrine

The [ANSSI's recommendations](#) help entities choose suitable cloud solutions based on system type, data sensitivity, and threat level. They advise conducting risk analyses, selecting appropriate security mechanisms, and ensuring team training to manage cloud migrations securely and minimize reliance on a single provider.

The ANSSI's recommendations are based on the **sensitivity of information systems**. Each system type requires different SecNumCloud-certified solutions, with non-commercial and private offers often preferred to prevent lateral attacks. For highly sensitive systems, the hosting decision must be based on a detailed risk analysis.

## Practical sheets on cloud computing services

The CNIL has received many questions about the use of cloud computing services, particularly in view of the complexity of the offers available. In response, [the CNIL has published two initial fact sheets](#).

In a [practical sheet on encryption](#), the CNIL offers a detailed analysis of the different types of **encryption** applied to cloud computing services, including encryption at rest, in transit, during processing, and end-to-end encryption.

In a [second fact sheet on security and performance tools](#) in the cloud, the CNIL presents the various security products needed to secure a cloud service. In doing so, it makes a clear distinction between security functionalities (anti-DDoS, WAF) and performance functionalities (CDN, Load balancers), which are often marketed together.

## The ANSSI and BSI publish a report on remote identity verification

### The ANSSI and the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) have published their sixth joint annual report, dedicated to remote identity verification.

The [ANSSI and BSI stated that digital transformation in Europe enhances citizens' identities through digital identification technologies, enabling access to various services](#).

The eIDAS regulation requires EU member states to issue digital identity wallets, and enrolment often involves video-based remote identity proofing. However, according to the ANSSI and BSI this method poses risks, including identity theft through presentation and injection attacks, which exploit system vulnerabilities.

In order to ensure authenticity, necessitating robust standards to maintain security and user trust, the ANSSI strongly **recommends effective remote identity proofing relies on biometric checks, document verification, and high video quality to ensure authenticity**, necessitating robust standards to maintain security and user trust.

Remote identity proofing utilizes methods like photo, video, or chip reading to capture identity documents, each vulnerable to counterfeiting and data injection.

The effectiveness of verification hinges on document security features, which differ by country. Chip reading is the most secure, but legal restrictions limit access to biometric data in the EU. The ANSSI says that attackers can exploit weaknesses in biometric algorithms, emphasizing the need for continuous evaluation and security measures.

While standardization efforts are growing, few certification schemes exist. As European digital identity wallets emerge, ensuring secure remote identity proofing is crucial to prevent identity theft and establish consistent security across Europe.





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

### The ANSSI publishes its safety recommendations for a Generative AI system

The [document](#) aims to raise awareness of the risks associated with Generative AI, and to promote best practices in the implementation of this type of system

According to ANSSI, the implementation of Generative AI systems involves three phases: training, integration and deployment, and operational production.

Each phase requires **tailored security measures** based on data sensitivity, subcontractor roles, and the AI system's criticality.

The ANSSI highlights that Generative AI systems face specific security risks, such as adversarial attacks and data exfiltration.

Protecting training data is crucial, and **user access must be restricted** to necessary information.

The ANSSI also stresses **avoiding public tools for handling sensitive data**. Confidentiality, integrity, and availability are essential, with secure and limited interactions between AI systems and other applications.

**Human oversight** is needed, especially for critical systems.

AI-assisted development requires close monitoring and regular testing to ensure security.

Finally, ANSSI recommends protecting AI models to safeguard national assets and prevent attackers from exploiting model architectures for malicious purposes, such as enhancing attacks or stealing data.

### The ANSSI and BSI publish their security recommendations for AI-based programming assistants

This document provides [recommendations](#) for the safe use of AI-based programming assistants

AI coding assistants, powered by Generative AI and large language models (LLMs), are transforming software development by **automating code generation**. According to the ANSSI and BSI, these tools allow users to input natural language prompts, producing functional code across various programming languages.

While effective for basic tasks, their performance diminishes with complexity in large codebases. ANSSI and BSI note that **AI assistants streamline debugging, improve test case generation, and enhance documentation**.

Although user surveys suggest increased productivity, conclusive evidence of major gains is limited. **Security risks, such as the exposure of confidential information in training data, are a key concern**.

Companies should restrict access to AI tools and use secure accounts, while developers need **training to critically evaluate AI outputs**.

Supply chain attacks and data poisoning also require thorough code reviews, library validation, and proper documentation.

ANSSI and BSI recommend limiting extensions and conducting risk analyses to ensure responsible AI integration in software development.

## Ensuring responsible deployment that respects data protection

### The CNIL published guidance to help organizations responsibly deploy Generative AI systems while respecting data protection

The development of AI models requires training on vast amount of data which often contain personal information. Therefore, measures must be taken to **ensure compliance with data protection regulations**.

Many organizations are seeking guidance from the CNIL on how to deploy Generative AI systems, particularly concerning compliance with data protection rules. To help, [the CNIL offers a set of recommendations aimed at responsible and secure implementation](#):

- **Address specific needs:** Deploy systems with clear and predefined use cases;
- **Regulate usage:** Define permitted and prohibited uses, particularly avoiding imputing personal data into these systems or relying on them for decision-making;
- **Acknowledge system limitations:** Ensure users are aware of the potential risks to individuals rights;
- **Choose secure systems:** Prefer localized and secure systems or assess the third-party provider's ability to reuse input data;
- **Train users:** Educate users about prohibited uses and potential risks; and
- **Implement governance:** Ensure compliance with GDPR by involving key stakeholders early, such as data protection officers.

The CNIL continues to publish recommendations and [Q&As](#) and has launched consultations to address the complex issues surrounding the development and fine-tuning of AI systems.

## Continuing work to develop innovative and privacy-protective AI

### The CNIL's public consultation on AI system development guidelines highlights how GDPR supports responsible AI innovation

The CNIL, [continues its efforts to develop innovative AI while ensuring privacy protection](#). In July 2024, the CNIL submitted new guidance on AI development for public consultation, highlighting how the GDPR fosters responsible AI practices.

Since 2022, the adoption of AI technologies has surged across sectors like healthcare and public services, making **legal and ethical frameworks increasingly important**.

While AI is key to France's competitiveness, the CNIL emphasizes that development must occur within a framework that protects fundamental rights.

The CNIL **launched a second public consultation** (now closed) to address issues such as web scraping, open-source AI models, and individual data rights, seeking to provide legal clarity to stakeholders.

Throughout its consultations with various industries, the CNIL identified "**legitimate interest**" as a common legal basis for processing personal data in AI development, though it requires thorough risk assessments.

The CNIL also stresses the **importance of transparency and safeguarding individual rights**, particularly concerning data access and correction. Open-source AI models are seen as beneficial for transparency, but they also pose risks, such as security concerns and malicious use.

Overall, the CNIL's work seeks to ensure that AI systems are developed ethically, with privacy considerations at the forefront, thus fostering public trust in these technologies.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Adoption of the NIS2 Directive Transposition Law in French law

The transposition of the EU directive in France was initially scheduled for 18 October 2024 but following the dissolution of the National Assembly during the summer, the government only [recently presented the bill on "resilience of critical infrastructures and reinforcement of cybersecurity"](#) to the Council of Ministers.

This bill aims to **enhance national measures to secure vital activities and combat cyber threats by transposing three key regulations: the NIS2 Directive, the Digital Operational Resilience Act (DORA), and a directive to harmonize existing laws with DORA**. While the draft law has not yet been definitively adopted, it will notably outline the scope of essential and important entities based on effective criteria, minimum turnover, or balance sheet requirements, thereby addressing critical infrastructure resilience and cybersecurity needs.

## (Closed) New public consultation on the development of AI systems

On 1 October 2024, [the CNIL concluded its second public consultation](#) on practical sheets for artificial intelligence development, following an initial consultation in April 2024.

This round introduced five **new practical sheets** that expand upon key principles such as legitimate interests, data subject rights, and security.

The new sheets include relying on **legitimate interests as a legal basis for AI systems** (with two focus sheets on open-source models and web scraping data collection), guidelines for **informing data subjects** and ensuring their **rights** are respected, **annotating data** and ensuring the **security of AI development**.

These updates aim to provide clarity on data protection and enhance compliance within the evolving landscape of AI technology.

## (Closed) Public consultation conducted by the CNIL to contribute to the development of health-related frameworks

The CNIL [launched a public consultation](#), that closed on 12 July 2024, to update health data frameworks in collaboration with relevant stakeholders. This initiative evaluates reference methodologies MR-001 to MR-008, which focus on health data warehouses, prevention programs, and access protocols.

This consultation addresses new European regulations related to **clinical trials and medical devices**, as well as the **growing use of artificial intelligence in health data processing**. Stakeholders, including researchers and healthcare professionals, are encouraged to provide feedback, which will help the CNIL enhance health data methodologies, prioritize individual privacy rights, and support innovation. Ultimately, the consultation aims to create frameworks that comply with regulations while fostering advancements in health data management.

## (Closed) Public consultation by the CNIL on a draft recommendation for measuring workplace diversity

The CNIL [launched a public consultation](#), which closed on 13 September 2024, on a draft recommendation aimed at guiding organizations in **measuring workforce diversity while complying with privacy regulations**, particularly the GDPR. Given the sensitive nature of data such as health status, sexual orientation, and perceived ethnic origin (the collection of which is generally prohibited) the CNIL emphasizes the need for **voluntary participation and informed consent**.

The draft recommends using anonymous surveys and limiting data collection to closed questions. To address potential participation issues due to employer-employee dynamics, the CNIL suggests utilizing a **trusted third party** for data collection.



# Germany

## Contacts



**Nikola A. F. Werry**

Partner, Deloitte Legal Germany  
[nwerry@deloitte.de](mailto:nwerry@deloitte.de)



**Dr. Till Contzen**

Partner, Deloitte Legal Germany  
[tcontzen@deloitte.de](mailto:tcontzen@deloitte.de)



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

## **Amendment of the German Federal Data Protection Act**

In 2018, together with the General Data Protection Regulation (GDPR), the new German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG-neu) came into force. After evaluating the BDSG-neu over the years, in February 2024, the federal government passed an [amendment to the BDSG-neu](#).

The proposed legislation seeks to incorporate key elements from the coalition agreement, as well as the findings from the evaluation of the Federal Data Protection Act (BDSG). A significant amendment is the introduction of Section 16, which formally establishes the Data Protection Conference—a body consisting of independent federal and state data protection authorities—within the revised BDSG (BDSG-neu).

The next step is to publish the approved government draft.

## **Draft law amending Federal Criminal Police Office regulations for comparing biometric data with online public data**

The German government has introduced a package of measures aimed at enhancing national security. Among these is a draft bill proposing the integration of a '[comparison of biometric data with publicly available data from the internet](#)' into the Federal Criminal Police Office Act.

Notably, the legislation does not permit real-time biometric searches. The Federal Commissioner for Data Protection and Freedom of Information has raised concerns, citing several unresolved data protection issues related to the proposal.

## **Bavarian Data Protection Authority ordered to take action**

In a landmark ruling on 12 June 2024, the Administrative Court of Ansbach reinforced the crucial role of data protection supervisory authorities in enforcing data subjects' rights under Article 15 of the GDPR. The judgment emphasizes the authority's duty to act and implement appropriate remedial measures when data protection violations are identified.

Case summary: An attendee of a seminar requested comprehensive details from the event organizer about her stored personal data, including the purpose of processing and any data recipients. This request followed the organizer's distribution of a participant list containing room booking details. Dissatisfied with the organizer's response, the attendee filed a complaint with the Bavarian Data Protection Authority. The authority merely requested that the organizer provide the requested information, and the organizer claimed to have deleted the data. The court ruled in favor of the complainant, determining that the data protection authority was required to take action against the organizer. A simple statement from the organizer was deemed insufficient to resolve the complaint.

This ruling sets a precedent and strengthens the protection of personal data.

## **Change of the Federal Commissioner for Data Protection and Freedom of Information**

On 3 September 2024, Prof. Dr. Louisa Specht-Riemenschneider assumed her role as the new Federal Commissioner for Data Protection and Freedom of Information. Along with this leadership transition, a shift in key focus areas is anticipated. The agenda is expected to broaden, with increased emphasis on artificial intelligence, healthcare, and security, as well as enhanced collaboration between data protection authorities in the future.

# ? What are the most relevant **cybersecurity updates?**

## **Implementation of the NIS2 Directive (EU) 2022/2555 in Germany**

The EU's NIS2 Directive must be incorporated into national law by October 2024. The government draft for implementing the NIS2 Directive ([NIS2UmsuCG](#)) and enhancing cybersecurity was adopted on 24 July 2024.

As of now, the law has not yet been officially promulgated and it is expected that Germany will miss the deadline, likely only transposing the NIS2 Directive by March 2025. The NIS2 Implementation Act will also revise the Act on the Federal Office for Information Security. A key focus of this act is the introduction of establishment categories outlined in the NIS2 Directive, marking a substantial expansion of the scope beyond essential service providers (KRITIS) and digital service providers. The Federal Office for Information Security (Bundesamt für Sicherheit und Informationstechnik, or BSI) expects that 30,000 entities will be covered by the transposition law in Germany alone, a significant increase from the 1,000 entities that were previously covered by NIS1.

Under the NIS2 Implementation Act, the BSI will receive additional responsibilities and powers. These include monitoring compliance, developing criteria, processes and tools to evaluate the security of IT Systems and components, providing business advice, facilitating coordination between authorities and industry, and enforcing sanctions. The NIS2 Directive mandates a stringent reporting obligation for significant IT security incidents, with the BSI tasked with defining and overseeing the reporting framework. Moreover, the BSI will conduct training initiatives and awareness campaigns to ensure that affected companies are informed of their obligations under the NIS2 Directive.

## **Strengthening the security and technological sovereignty of German 5G mobile networks**

The German government has reached agreements with telecommunications companies Telekom, Vodafone, and Telefonica, establishing that components from Huawei and ZTE must not be utilized in 5G core networks by the end of 2026 at the latest. Additionally, the critical management systems of these two suppliers in the 5G access and transport networks are required to be replaced with technology from alternative providers by the end of 2029.

Through these measures, the federal government aims to enhance the protection of critical infrastructure, such as public 5G mobile networks, against cyber attacks and to decrease reliance on individual suppliers.

## **How AI is changing the cyber threat landscape**

In a recent [research paper](#), the Federal Office for Information Security (BSI) examined the impact of artificial intelligence on the current cyberthreat landscape.

The study highlights how cyberattacks are evolving due to the advent of new technologies. Specifically, it focuses on large language models (LLMs), which lower the barriers to entry for cyberattacks while simultaneously amplifying the potential impact of malicious activities. However, the research indicates that fully autonomous malicious AI agents capable of executing attacks do not currently exist and are unlikely to emerge in the near future.

Conversely, cyber defenders also gain from increased productivity through the application of AI, particularly in areas such as malware detection. The BSI plans to provide further insights on this topic in an upcoming article based on its findings.



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

## **The Data Protection Conference publishes guidelines on artificial intelligence and data protection**

The Data Protection Conference, which comprises independent data protection supervisory authorities from both the federal and state levels in Germany, regularly publishes guidelines, application notes, and orientation aids pertaining to data protection. In May 2024, the Data Protection Conference released a [guide to artificial intelligence and data protection](#) on its website. This guide is intended to assist in the selection, implementation, and use of AI applications in compliance with data protection regulations. It primarily focuses on large language models (LLMs), which are often employed as chatbots. The guidance is primarily aimed at decision-makers who wish to leverage AI technologies.

## **Federal Office for Information Security publishes a research paper on the topic: Transparency of AI Systems**

In July 2024, the German Federal Office for Information Security released a [research paper](#) titled "Transparency of AI Systems." The paper underscores the critical importance of transparency in both the AI Regulation and the GDPR. It explores the concept of transparency and establishes its connection to the requirements outlined in the AI Regulation. Additionally, the research paper discusses the opportunities and risks associated with (transparent) AI systems. The benefits of transparency include the early identification of potential risks or vulnerabilities and undesirable effects, as well as enhanced traceability of decisions. Conversely, a significant risk associated with disclosing information about the functioning of AI systems is the potential creation of new vulnerabilities that could be exploited for malicious purposes.

## **Proposal on national responsibilities for the AI Regulation from the Data Protection Conference**

In response to the new European Artificial Intelligence Act (AI Act), member states are required to establish a regulatory oversight structure within 12 months of its entry into force. The Data Protection Conference believes it would be beneficial to designate [national data protection authorities as market surveillance authorities under the AI Act](#), given their extensive experience, independence, and established cooperation and coherence mechanisms. Furthermore, the Conference suggests that the Federal Commissioner for Data Protection and Freedom of Information should also be appointed to this role. Collaboration among these organizations as market surveillance authorities is regarded as highly advantageous.

However, the financial sector and critical infrastructure should be excluded from national competencies. Due to their significant importance, distinct responsibilities would need to be established within Germany for these sectors.

## **Discussion paper by the Hamburg Commissioner for Data Protection and Freedom of Information on LLMs**

In July 2024, the Hamburg Commissioner for Data Protection and Freedom of Information published a [discussion paper](#) on the topic of "LLMs and personal data". The paper is intended to serve as a guide for companies and authorities. The Commissioner states that storing an LLM without personal data isn't considered processing under GDPR and that compliance with GDPR, including data subject rights, is mandatory when personal data is processed within an LLM-based AI system. While the LLM itself doesn't comprise personal data, rights like access and deletion apply to the inputs and outputs of such AI systems.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Employee Data Protection Act

A new independent law on employee data protection was anticipated in 2024. To date, employee data protection has only been addressed within the framework of the Federal Data Protection Act.

The forthcoming Employee Data Protection Act is being developed collaboratively by the Federal Office of Labour and Social Affairs and the Federal Ministry of the Interior and Community, in accordance with the coalition agreement. As a preliminary step, the ministries have produced a joint document outlining proposals for a total of 12 regulatory areas within the independent law.

Calls for an independent employee data protection law have persisted for decades, and it is expected that such legislation may be enacted by 2025.

## Applicability of EU regulation

Several EU regulations will take effect in 2025.

Among these is the EU AI Act. While full applicability is not anticipated until two years after its entry into force in 2026, the prohibition on AI systems that pose unacceptable risks will be enforced as early as February 2025.

Additionally, the Data Act will be directly applicable in all EU member states by 2025. The primary objective of the Data Act is to promote fair data use and equitable access to data within the European Union.



# Ghana

## Contacts



**Wisdom Kpano**

Associate Director, Deloitte Ghana  
[wkpano@deloitte.com.gh](mailto:wkpano@deloitte.com.gh)



**Naa Adzorkor Adzei**

Manager, Deloitte Ghana  
[nadzei@deloitte.com.gh](mailto:nadzei@deloitte.com.gh)

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

## **Scaling up of Enforcement of Specific Provisions of the Data Protection Act 2012 (Act 843)**

In July 2023, the Data Protection Commission of Ghana announced its decision to scale up enforcement of the Data Protection Act 2012 (Act 843), in the following areas:

- Mandatory registration of data controllers with the Data Protection Commission;
- Renewal of registration with the Commission every two years;
- Imposition of penalties for failure to register with the Commission. The penalties applicable are a fine of up to GHS 3,000 or a term of imprisonment of two years or both;
- Prohibition against requesting for particular records as a condition for the provision of goods or services unless required by a specific law or in the public interest. The penalty for failing to comply with this prohibition is a fine of up to GHS 3,000 or a term of imprisonment of two years or both; and
- Protection against the sale, purchase or disclosure of personal data. Penalty for contravention of this provision is a minimum fine of GHS 3,000 or a term of imprisonment of two years or both.

## **Technology policy framework reform**

In December 2023, the Ministry of Communications and Digitization announced that the Ghana Information Communication Technology Policy, launched in 2003, will be replaced by a Ghana Digital Economy Policy (the Digital Economy Policy).

The Digital Economy Policy will focus on digitalization to drive significant change in three technology ecosystems:

- Government ecosystem;
- Private sector ecosystem, and citizens, residents; and
- Global community ecosystem.

The policy will anchor on strengthening and developing the three technology ecosystems. It is expected that once the policy is launched, through new and enhanced efforts, existing legal shortcomings will be easily identified and addressed, paving the way for the enactment of relevant and effective legal frameworks.

The policy is intended to also cover vital areas of the Ghanaian digital economy such as digital Infrastructure, data-driven innovation, entrepreneurship, data protection, user privacy, cybersecurity, and digital literacy and skills.

## Technology policy framework reform

In November 2023, the Ministry of Communications and Digitalization (MOCD), in collaboration with the Ministry of Environment, Science, Technology & Innovation (MESTI) and GIZ Ghana launched the Ghana Digital Innovation Week (GDIW) with a goal of putting together the necessary policy instruments (the Digital Economy Policy) to address some market challenges.

GDIW will serve as opportunity to observe, assess and evaluate national readiness to participate in the digital economy.

## Duty to protect the data of data subjects

In September 2024, a circuit court determined that a data controller and a data processor have a duty to verify information submitted to them by a data subject and check the liveliness of that data subject.

Among other things, the court ordered the Data Protection Commission to ensure that all ride hailing entities in Ghana undergo a forensic audit exercise and conduct a liveliness test for data on drivers who use their platforms for a specified period.

## Admissibility of digital evidence in Ghana's courts

In 2016, digital evidence was admitted for the first time in Ghanaian courts. The court established that digital or electronic evidence will be admitted as evidence if:

- The court is satisfied with the reliability of the electronic evidence;
- Digital forensic experts authenticate the evidence; and
- The integrity of the evidence is maintained.

In the same year, the courts decided that the balancing doctrine must be employed, meaning data presented in courts as evidence must not breach one's fundamental rights.

# ? What are the most relevant **cybersecurity updates**?

## Cyber Security Authority - Cybersecurity Act 2020 (1038)

### Relevant updates

- In September 2024, Ghana was ranked a tier one status globally for being a role model country for cybersecurity development in the latest International Telecommunication Union (ITU) Global Cybersecurity Index (GCI). Ghana scored a 99.27% making Ghana, the second highest scoring country on the continent after Mauritius.
  - The score of 99.27% indicated that Ghana improved upon its ratings under the different pillars compared to the 2020 GCI rankings in which Ghana was rated at 86.69%, placing it third in Africa after Mauritius and Tanzania.
  - The authority has also identified the need to enhance the capabilities of the National Computer Emergency Response Teams (CERTs) to combat cybercrime.
  - In September 2022, Ghana was recognized as a hub for training and capacity building for the sub-region by entities such as the European Union, Council of Europe (COE), the World Bank, and ECOWAS.
  - In August 2024, Ghana ratified the Second Additional Protocol to the Budapest Convention and other international cooperation engagements.
  - On 8 August 2024, Ghana significantly contributed to discussions on the adoption of the recent UN Convention on Cybercrimes which is the first global legally binding instrument on cybercrime.
- Ghana cybersecurity services licensing:
    - In March 2023, Ghana's Cyber Security Authority launched a new system of licensing for companies and professionals that provide cybersecurity-related services in Ghana in line the country's Cybersecurity Act 2020 (Act 1038).
    - The licensing regime, which became effective from September 2023, creates three separate categories: cybersecurity service providers (CSPs), cybersecurity establishments (CEs) and cybersecurity professionals (CPs).
    - As of July 2024, the authority announced that a total of 51 CSPs, CEs, and CPs had received licenses and accreditation.
    - Failure to comply with the licensing regime may result in monetary penalties for defaulting entities and professionals.
  - 
  -





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

## AI updates in Ghana

- In June 2024, the African Information and Communications Technology (ICT) and Communications Ministers approved the AU Continental Artificial Intelligence strategy, and the AU Executive Council subsequently approved it in July 2024.
- Ghana has since incorporated the African Union AI strategy into its national AI strategy 2023.
- The government of Ghana is investing in AI infrastructure and areas identified by the AU Continental AI strategy by specifically focusing on:
  - Digital literacy;
  - Training programs; and
  - Physical infrastructure.
- The training programs are focused on diversity and developing a more equitable workforce. For example, Ghana Tech Lab supports women enrollment in AI training programs. Similarly, the Ministry of Communication launched a program called 'Ms. Geek', aimed at increasing gender diversity in STEM. Other initiatives include an all-women technology lab launched in 2016 to advance women-led technology businesses.
- Ghana has developed a National Artificial Intelligence Strategy, through the Ministry of Communication and Digitization with support from Smart Africa, GIZ Fair Forward, The Future Society and some stakeholders of Ghana's AI ecosystem.
- The goal of the National Artificial Intelligence Strategy is to serve as a comprehensive roadmap for harnessing the potential of AI's application to accelerate the country's inclusive and sustainable socio-economic development and mitigate the risks that come with AI adoption and use.
- Since 2019, the Ministry of Health in collaboration with a private sector entity, has been delivering medical supplies to health centers in rural areas using drones



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Expected developments in Ghana

### Artificial intelligence

- Ghana's 2023 AI strategy addresses the development of AI-powered digital health infrastructure and interoperability systems. For instance, the generation and integration of electronic medical files of patients into single digital health records accessible for timely use by authorized healthcare facilities and medical practitioners in different parts of the country is expected to improve healthcare delivery in the near future.
- Integration of AI tools and technologies in the agricultural sector will optimize irrigation to increase food production as well as enhance the storage and preservation of food produce.
- Integration of AI in agriculture would also ensure that there is all-year round farming which can boost the availability of food in high supply to meet the raw material demands of food processing industries and the nutritional needs of Ghanaians. This could also reduce the phenomenon of post-harvest losses and increase the incomes of farmers.
- Ghana will be focusing on practical applications of AI in the education sector. This will include concepts of AI ethics and techniques, programming and algorithmic thinking.
- Ghana will also be [integrating AI competencies into STEM education](#).
- Ghana is also expected to launch its Ghana Digital Economy Policy soon which will replace the Ghana Information Communication Technology Policy.

### Cybersecurity and data protection

- Ghana's government is working towards a working database that accurately captures personal biodata of the population. This will aid the efforts of the police and the Cybersecurity Authority in solving cybercrimes. The database can effectively be tapped into for use in AI systems.
- AI-powered tools will be used to detect and respond to cyber threats more effectively, including anomaly detection, threat intelligence, and incident response.
- Government and private organizations will continue to raise awareness about cybersecurity risks and best practices among the general public.
- As AI becomes more prevalent, Ghana is expected to focus on developing guidelines to address the ethical and legal implications of AI-driven data processing, including bias, accountability, and transparency.
- Ghanaian government is working on a legal framework that is relevant to the Digital Economy Policy goal attainment, digitalization, and transformational impact. The legal framework is expected to be passed in 2024.
- Ghana's Cybersecurity Authority will continue to enforce the licensing and accreditation regime for entities and professionals providing cybersecurity related services in Ghana.

# Greece

## Contacts



**Arianna Sekeri**

Partner, KBVL Law Firm (member of the Deloitte Legal network)

[asekeri@kbvl.gr](mailto:asekeri@kbvl.gr)



**Maria-Alexandra Papoutsi**

Managing Associate, KBVL Law Firm (member of the Deloitte Legal network)

[mapapoutsi@kbvl.gr](mailto:mapapoutsi@kbvl.gr)

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

## **Hellenic Data Protection Authority's Opinion on the draft law on measures for the implementation of Regulation (EU) 2022/2065 (DSA)**

The Greek Ministry of Digital Governance submitted a request to the Hellenic Data Protection Authority (HDPa) for its opinion on the draft law implementing Regulation (EU) 2022/2065 on the Digital Services Act (DSA) for the single market. The HDPa's opinion includes both general observations and specific comments on the draft law's provisions.

Key points highlighted by the HDPa include:

- Its designation as the competent authority for supervising intermediary service providers and enforcing Articles 26(1)(d), 26(3), and 28 of the DSA;
- Provisions for cooperation, mutual assistance, and information exchange between the Digital Service Coordinator and relevant authorities;
- The process for imposing fines and periodic penalties; and
- The clause allowing a derogation from the general rule that acts of the HDPa are subject to judicial review solely through an application for annulment before the Council of State.

## **Hellenic Data Protection Authority's Opinion on the Presidential Decree provided in Article 107, paragraph 6 of Law 4727/2020 regarding the Citizens' Personal Number**

The Greek Ministry of Digital Governance has submitted a draft presidential decree for the authority's opinion, as provided in Article 107(6) of Law No. 4727/2020, concerning the Citizens' Personal Number (PN). The authority's opinion includes both general and specific comments on the provisions of this draft.

Key issues highlighted by the HDPa include:

- The significance of the Personal Number (PN) as a critical service component for authenticating individuals within public sector bodies. The PN Register facilitates linking PNs to each entity's sectoral identifiers, thereby enabling precise citizen identification through a memorable number.
- The level of protection afforded to the PN as personal data, given that it is not included in any official public document.
- In line with the principle of data minimization, the necessity of a long-term strategy to:
  - Adapt public registries to a single sectoral identifier per entity. This includes redesigning applications in cases where multiple identifiers are currently used, to eliminate unnecessary ones; and
  - Restrict, as per the Ministry of Digital Governance's planned timeline, the transmission of sectoral identifiers that differ from those corresponding to each entity's sector.
- The rejection of the argument that processing the PN facilitates interoperability within public sector information systems. The sole purpose served is to provide identity verification services for natural persons to public sector bodies.



### **Decision [09/2024](#): Promotional phone calls made by a Greek energy provider and its partner call centers**

The HDPa conducted a joint examination of numerous complaints regarding promotional phone calls made by a Greek energy provider, lasting over two years. Following the analysis of the company's activities and those of five collaborating call centers, a fine of €127,709 was imposed on the provider due to deficiencies in the oversight of its partners.

Additionally, three call centers were fined €10,000, €6,000, and €20,000, respectively, for security violations during the phone calls. One of them was also penalized €5,000 for collecting phone numbers in violation of the GDPR. The HDPa implemented corrective measures to ensure the legality of their processes.

### **Decision [10/2024](#): Leak of personal data subsequently published on the dark web**

The HDPa imposed a fine of €2,995,140 on a data controller following a personal data breach, which subsequently led to the publication of the leaked data on the dark web. The investigation revealed that the data controller failed to implement the necessary technical and organizational measures and did not ensure the enforcement of its security policy for data processing.

This resulted in actions during the breach, including network vulnerability scanning, unauthorized access to resources, execution of malicious processes on workstations, disabling of security software, and encryption of files.

### **Decision [13/2024](#): Self-investigation for the development and implementation of the "Centaurus" and "Hyperion" programs by the Ministry of Immigration and Asylum regarding the control of reception and accommodation facilities for third country nationals**

The HDPa, after reviewing the implementation of the "Centaurus" and "Hyperion" programs by the Ministry of Migration and Asylum at Closed Controlled Structures and Reception and Identification Centers for third-country nationals, conducted a thorough inspection of the integrated digital system for managing electronic and physical security – "Centaurus" – and the access control system using biometric data – "Hyperion."

The authority found the ministry, as data controller, inadequately cooperative and determined that the ministry's Data Protection Impact Assessments (DPIAs) were fundamentally insufficient and narrow in scope.

Additionally, significant non-compliance issues with specific GDPR provisions regarding the implementation of these systems were identified. Consequently, the authority imposed an administrative fine of €100,000 on the ministry for violations related to its cooperation with the HDPa and the DPIAs, while also issuing a compliance order with a three-month deadline to meet its obligations under the GDPR.

### **Decision [23/2024](#): Fine and compliance order issued to EKAB for violation of access rights to recorded calls**

The HDPa reviewed complaints regarding the National Emergency Assistance Center's (NEAC) refusal to provide access to recorded calls on the 166-emergency line, citing inability to identify callers. It found NEAC in violation of the GDPR, recognizing that callers are identifiable and imposing fines totaling €30,000-€20,000 for infringing the complainants' access rights and €10,000 for lack of transparency. NEAC was ordered to amend its policy to evaluate identification on a case-by-case basis, ensuring rights to access recorded calls are not blocked by default.

### **Decision [32/2024](#): On the new type of identity cards for Greek citizens**

The HDPa reviewed issues arising from the issuance of new ID cards for Greek citizens, identifying deficiencies in general information provided to data subjects and delays and gaps in the required Data Protection Impact Assessment (DPIA). Consequently, a fine of €150,000 was imposed on the Ministry of Citizen Protection, the data controller, for these violations, along with an order to comply within six months. The authority also emphasized the need to update and codify the legal framework governing the elements included in the new ID cards for Greek citizens.

# ? What are the most relevant **cybersecurity updates**?

## Draft law for the implementation of the NIS2 Directive

### Public consultation process

The **Greek Ministry of Digital Governance** has recently released a **draft law** that aligns with the EU's Directive (EU) 2022/2555 (NIS2). Currently under **public consultation** until 2 November 2024, this legislation seeks to establish a more robust and unified cybersecurity framework in Greece.

The proposed draft law covers gaps identified during the application period of NIS Directive 1, which was transposed into Greek law with Law No. 4577/2018:

- In the **definition of cybersecurity risk management measures and incident reporting obligations** across all sectors it covers, such as energy, transport, health, public administration, supply chain, food production, telecommunications, and digital infrastructure; and
- In the **uniform handling** of relevant issues across all member states of the EU.

Specifically, the law introduces the following measures:

- **National cybersecurity strategy:** Establishes a clear national approach to cybersecurity by designating a specific authority responsible for cybersecurity policies, crisis management, and coordination.
- **Comprehensive risk management protocols:** Mandates specific cybersecurity risk management standards, aiming to strengthen cyber defenses and minimize vulnerabilities.

- **Enhanced information sharing:** Sets protocols to facilitate secure and effective information exchange between public and private entities, crucial for coordinated responses to cyber threats.
- **Supervision and enforcement mechanisms:** Lays out a framework for the supervision and enforcement of cybersecurity compliance across sectors, focusing on critical infrastructure.

## Law No. 5086/2024: National Cybersecurity Authority

### Establishment of the Greek National Cybersecurity Authority

The **Greek Ministry of Digital Governance** officially published **Law No. 5086/2024** (Government Gazette 23' A/14 February 2024), establishing the **National Cybersecurity Authority**.

The structure of the law is as follows:

- **Chapter A** (Articles 1-2): Definition of the law's purpose and scope, laying the foundation for the new provisions.
- **Chapter B** (Articles 3-9): Establishment of the National Cybersecurity Authority as a public legal entity within the central government sector. Supervision responsibilities for cybersecurity policies and coordinating efforts across various sectors.
- **Chapter C** (Articles 10-15): Organizational structure of the National Cybersecurity Authority (e.g., Internal Units, Legal Counsel Office, Transfer of Personnel etc.).
- **Chapter D** (Articles 16-19): Amendments for the alignment with existing laws, following the establishment of the National Cybersecurity Authority.



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

## National Strategy on Artificial Intelligence

As part of its digital transformation program, also known as the [Digital Transformation Bible](#), the Greek government is actively developing a National Strategy on Artificial Intelligence. This strategy aims to create a comprehensive framework for the future development and implementation of AI in Greece.

It will be organized around a series of coordinated and interconnected actions, focusing on maximizing potential benefits while minimizing costs to the economy and society. This cohesive policy document will define the essential conditions for AI development, encompassing skill and trust frameworks, data policies, and ethical principles to ensure the safe use of AI. It will identify national priorities and areas for leveraging AI to tackle social challenges and drive economic growth.

Furthermore, the strategy will assess the necessary actions related to these priorities, recommending horizontal interventions and at least one pilot application within each policy sector.

## Land Registry: new AI tool for legal review purposes

Greece's Land Registry has become the first public agency to integrate AI into its legal review process. This innovative tool aims to revolutionize how contracts are processed. Previously, officials faced the task of reading contracts, taking an average of 30 minutes per document. The new AI tool streamlines this by reading contracts in natural language, identifying transaction types, and extracting essential legal elements. It also conducts completeness checks for compliance with tax and legal requirements while generating recommendations for contract approvals or rejections.

Early trials suggest that processing times could be reduced by more than half, significantly cutting costs from €15 to as little as €0.30 per contract. While final decisions remain with department heads, the AI tool provides valuable insights that enhance efficiency and accuracy in public service. Developed at no cost by the Ministry of Digital Governance using Microsoft Azure Open AI technology, this initiative exemplifies Greece's commitment to leveraging AI for smarter governance and improved public services.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## **Adoption of the law under public consultation on the transposition of the NIS2 Directive**

The upcoming adoption of the law for the transposition of the NIS2 Directive is a critical step in enhancing Greece's cybersecurity framework. Following the conclusion of the public consultation process on 2 November 2024, stakeholders will have provided valuable feedback that informs the final legislation. This phase is essential for ensuring that diverse perspectives are considered, ultimately leading to a more robust regulatory framework that addresses the challenges posed by cybersecurity threats.

Once introduced for discussion in the Greek parliament, the law will establish stricter security requirements for essential and important entities, aligning Greece with broader EU cybersecurity standards. This initiative not only aims to bolster the resilience of critical infrastructure against cyber incidents but also demonstrates the government's commitment to a proactive cybersecurity strategy, fostering public trust in digital services as threats continue to evolve.

# Guatemala

## Contacts



**Estuardo Paganini**

Partner, Deloitte Legal Guatemala  
[egpaganini@deloitte.com](mailto:egpaganini@deloitte.com)



**Manuel Lara**

Senior Manager, Deloitte Legal Guatemala  
[manlara@deloitte.com](mailto:manlara@deloitte.com)

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

## **Law on Access to Public Information (Decree 57-2008 of the Congress of the Republic)**

While Guatemala lacks specific legislation for personal data protection, provisions within the law on public records address data privacy and can apply to private entities.

This regulation defines personal data, sensitive personal data, and the National Data Protection Authority.

Article 64 prohibits private parties from commercializing personal data without consent. Violations may result in five to eight years of imprisonment, fines ranging from Q.50,000 to Q.100,000 and confiscation of any tools used in the commission of the crime.

## **Law of Acknowledgment of Electronic Communications and Signatures (Decree 47-2008 of the Congress of the Republic)**

Electronic marketing is not considered e-commerce, yet it is considered a communication and an electronic communication as it contains an exposition, statement, claim, advice, request, or offer and the acceptance of an offer, in relation to the construing or execution of a contract.

This helps to speed up the registration of companies, trademarks, modifications of companies.



# Hungary

## Contacts



**Dániel Nagy**

Managing Associate, Deloitte Legal Hungary  
[dnagy@deloittece.com](mailto:dnagy@deloittece.com)



**Flóra Szalai**

Senior Associate, Deloitte Legal Hungary  
[fszalai@deloittece.com](mailto:fszalai@deloittece.com)



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

## **Whistleblower Protection Act**

### **Act XXV of 2023 on Complaints and Public Interest Disclosures, and on the Rules of Whistleblowing Notifications**

In July 2023, the Act on the protection of whistleblowers, on the mechanisms through which individuals can raise concerns about misconduct, wrongdoing, or unethical practices within an organization became effective. The act serves the purpose of compliance with Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law.

For compliance with the act, employers who employ at least 50 employees need to establish a whistleblowing system to report potential breaches. Companies should also implement appropriate anonymization measures, and inform data subjects about the new data processing activity.

Within the framework of the internal breach reporting system, the personal data (i) of the reporting person, (ii) of the person whose conduct or negligence gave rise to the report, and (iii) of the person who may have relevant information about the contents of the report, may be processed to the extent absolutely necessary for the investigation of the report solely for the purpose of investigating the report and for remedying or eliminating the conduct that is the subject of the report. Data processed within the framework of the internal fraud reporting system may be forwarded to a third country or international organization only if the recipient of the transmission has made a legal commitment to comply with the provisions of the act.

## **Changes in connection with data erasure codes**

Pursuant to Government Decree No. 726/2020 (XII. 31.) on the Determination of Procedural Rules Related to the Provision of an Application Enabling Data to be Made Permanently Inaccessible, distributors of durable mediums (e.g., mobile phones and laptops) must claim data erasure codes from the National Tax and Customs Administration and provide the data erasure codes to consumers purchasing such durable mediums free of charge.

As a general principle, both distributors and providers of online invoicing programs will be jointly responsible for supplying data erasure codes to consumers. Specifically, distributors are required to mark durable mediums in a way that online invoicing program providers can automatically detect. Providers must ensure their service identifies the durable medium without human intervention and automatically delivers the data erasure code to consumers.

Distributors must also notify online marketplace providers that the item being sold is a durable medium. If they fail to do so, distributors will be held liable for supplying the data erasure codes to consumers.

## Beauty salon fined for unlawful monitoring

### NAIH-2732-2-2023

The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) held a beauty salon liable for major GDPR infringements including cameras monitoring employees and clients, the mishandling of sensitive data and the use of data for marketing purposes without proper consent. The NAIH imposed a fine of HUF 30 million (approx. €75,000).

The main findings were the following: (i) the cameras were monitoring the room where staff ate, the training rooms and customer treatment rooms (implying that clients were often seen in incomplete clothing) with unclear purpose; (ii) all clients had to fill in and sign a consultation form which mentioned the placement of cameras for the purpose of protecting clients and staff. It however did not mention the recording of audio; (iii) the controller stored health data in the client database, including COVID-19 vaccination status, pregnancy, and sicknesses without proper legal basis; and (iv) the controller stated that the signature of the consultation form constituted a consent to the processing of their data for a marketing purpose, however, there was no checkbox on the consultation form to consent to the processing for marketing purposes. The clients therefore did not consent to the processing for this purpose.

## Code of conduct on data protection aspects of taking pictures in healthcare institutions

The NAIH issued a notice regarding the data protection implications of taking pictures in Hungarian healthcare institutions.

NAIH clarified that recordings without personal data in state and local government-run healthcare institutions are public data, but their creation and processing fall under GDPR regulations. Individuals and organizations involved in managing, creating, or altering these recordings bear increased responsibility, especially when processing special data like images of patients, and must adhere to General Data Protection Regulation (GDPR) regardless of their status as representatives.

NAIH outlined that:

- State and local government-run healthcare institutions perform a public task, therefore, recordings made in such institutions, which do not contain personal data, are data of public interest and considered public data in the public interest;
- Creation, collection, storage, editing, or masking of such recordings before publication is considered data processing under the scope of the GDPR;
- Recording images of patients in medical institutions can also enable the processing of special data, therefore individuals determining the purpose and means of data management, as well as the individuals and organizations who create, transmit, edit, and mask such recordings, have increased responsibility; and
- The status of a representative does not mean additional data management rights - representatives must also comply with the GDPR.

# ? What are the most relevant **cybersecurity updates?**

## **Law for the implementation of the NIS2 Directive**

### **Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision**

The NIS2 Directive entered into force on 3 January 2023, while Act XXIII of 2023 was promulgated on 23 May 2023.

The deadline to comply with Act XXIII of 2023 was 28 October 2024. Inspection will be carried out and sanctions will be imposed in the event of non-compliance by the Regulated Activities Oversight Authority (SZFTH).

NIS2 and the Cybersecurity Act basically include information security requirements for organizations. The law requires the development and operation of an efficient and risk proportionate information security management framework. Compliance with regulations is to be audited every two years by an independent auditor. Audit is mandatory even if the organization concerned already has industry-specific certifications (e.g., TISAX, ISO27001) or other audits (e.g., SOC2). Although the audit is not replaceable, existing certifications will certainly be useful for preparations and future NIS2 audits.

In addition, organizations must develop an efficient, risk proportionate information security management framework until 18 October 2024. Organizations must also have an agreement with an auditor until specified deadlines. Businesses must complete the independent audit until 31 December 2025.

## **Additional cybersecurity requirements**

### **Decree No. 7/2024 (VI. 24.) of the Cabinet Office of the Prime Minister**

As part of the implementation of the requirements of NIS2, the Cabinet Office of the Prime Minister issued a decree on the requirements for security classification and the specific security measures to be applied for each security class.

The decree defines the following categories of protection measures: program management, access control, awareness and training, logging and accountability, evaluation, authorization and monitoring, configuration management, contingency planning, identification and authentication, security incident management, maintenance, media protection, physical and environmental protection, system and communications security, system and information integrity and supply chain risk management.



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

## Government decree adopting AI Act

The Hungarian government issued Decree No. 1301/2024 to implement the EU Artificial Intelligence Act, assigning an organization under the Minister of National Economy to handle notification, market surveillance, and regulatory test environments. Additionally, the Hungarian AI Council was established, comprising various national authorities and a private company, to issue guidelines and resolutions for the decree's implementation.

The decree outlined that the implementation will be ensured by an organization established under the supervision of the Minister of National Economy, and this organization will:

- Perform notification and market surveillance, ensuring the possibility of a one-stop-shop procedure and single-point-of-contact tasks under the EU AI Act; and
- Create and operate a regulatory test environment in accordance with the EU AI Act.

Furthermore, the decree established the Hungarian Artificial Intelligence (AI) Council, which is authorized to issue guidelines and resolutions related to the implementation of the decree and is composed of the following members:

- National Media and Communications Authority;
- Hungarian National Bank;
- Economic Competition Office;
- National Authority for Data Protection and Freedom of Information (NAIH);
- Supervisory Authority for Regulated Activities; and
- Digital Hungary Agency Private Limited Company.

## Artificial Intelligence Coalition and Strategy

The goal of the Artificial Intelligence Coalition (AI Coalition), initiated by Dr. László Palkovics, Minister of Technology and Industry, is for Hungary to be at the forefront of artificial intelligence developments and applications in Europe and to become an important member of the international AI community.

The intention of the founders of the AI Coalition was to establish a permanent professional and cooperation forum for AI developers, market and government actors representing the user side of AI, the academic sphere, professional organizations, in order to jointly define the directions and frameworks for the domestic development of artificial intelligence.

The AI Coalition together with the Ministry of Innovation and Technology (its successor: the Ministry of Technology and Industry) created [Hungary's Artificial Intelligence Strategy](#) for the period 2020-2030, which was adopted by Government Resolution 1573/2020 (IX.9). The coalition has started reviewing the strategy in accordance with its milestones.

The strategy goals up to 2030 and outlines a related action plan extending up to 2025. The strategy proposes the following main groups of measures: (i) foundation pillars to prepare society to manage inevitable changes resulting from AI effectively and to fully exploit the advantages of the technology; (ii) focus areas such as sectoral and technological priorities; and (iii) transformative programmes which are complex means-end schemes provided in a form that is readily comprehensible for society as a whole. The directions outlined here show the ambitious path Hungary is to take for the stakeholders of both the Hungarian and international AI ecosystems.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Digital Citizenship Programme (DAP)

The Hungarian government is launching its digital citizenship program starting from 1 September 2024. The main goal of the initiative is to conduct more of the citizens' administrative errands digitally; and not to have to rely on physical copies of the individuals' paperwork.

The new system will offer two types of administrative procedures: one based on life events and the other on e-paper. The latter already exists; however, it will go through a complete overhaul. In case of the life event based administrative procedure, the most common cases are related to birth and car transfer, which are planned to be available as early as 2025.

Each Hungarian citizen's social security (TAJ) number, the number assigned to them in the public health care system, will be available in a mobile app, and so will be their personal ID number, and the registration of their vehicles. The program will enable personal identification, electronic signature compliant with eIDAS legislation and conducting a part of personal business for citizens by using their mobile phones. The DAP will later ensure them safe digital access and use of state and market services and the payment of public utility bills.

The circle of digitally accessible services will be significantly expanded in 2025 and, in a consecutive phase, in 2026. The DAP is a cloud-based application and optional for citizens of Hungary as the older, conventional methods for using services will also remain in place.

# Iceland

## Contacts



**Haraldur Ingi Birgisson**

Partner, Deloitte Legal Iceland  
[haraldur.ingi.birgisson@deloitte.is](mailto:haraldur.ingi.birgisson@deloitte.is)



**Alma Tryggvadóttir**

Director, Risk Advisory, Deloitte Iceland  
[atryggvadottir@deloitte.is](mailto:atryggvadottir@deloitte.is)

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

## **Simplified handling of complaints by the Icelandic Data Protection Authority**

In March 2023, changes were made to Act 90/2018 on privacy and the processing of personal data with the aim of simplifying the handling of complaints by the Icelandic Data Protection Authority (Persónuvernd) to reduce the workload of the authority, shorten processing times, and increase efficiency in case management. In each case the authority will assess whether a complaint will be investigated and ruled on or resolved in a simpler way. Additionally, DPA can refuse to handle a complaint e.g., if there is little likelihood of a violation or if the same issue has been resolved previously according to the authority's updated procedural rules.

## **New regulation on the processing of information about financial matters and creditworthiness**

Icelandic data protection legislation requires a regulation be set further specifying the processing of information concerning the financial matters and creditworthiness of individuals and legal entities, including debt registration and creditworthiness assessments, for the purpose of sharing it with others. The current regulation 246/2001 was issued based on Directive 95/46/EU and was updated to in accordance with the great accountability of controllers according to the General Data Protection Regulation.

## **Audits on the use of cloud services in elementary schools**

Persónuvernd issued five rulings regarding the use of Google's student system where various violations of data protection legislation were found. These were part of a broader project initiated by the European Data Protection Board and a part of the authority's inspection plan for 2022.

## **Public online health portal fined for security breach**

Persónuvernd imposed a ISK 12 million (approx. €78,475) administrative fine on the Icelandic Directorate of Health after the Directorate had reported a security breach regarding Heilsuvera, an online health portal that provides access to various health-related services, after two individuals had access to sensitive personal data not related to them.

## **Municipality of Reykjavík fined for the use of Seesaw student system in elementary schools**

Persónuvernd imposed a ISK 5 million (approx. €33,000) administrative fine on the municipality of Reykjavík regarding the processing of personal data by the municipalities' elementary schools in the Seesaw student system. The investigation revealed various violations through the use of the system.

## **District Court ruling on the Icelandic DPA's decision against Reykjavík municipality**

Reykjavík municipality initiated proceedings against the Icelandic Data Protection Authority in case E-4081/2023 concerning the authority's decisions on the unlawful processing of personal data in the Seesaw student system. In February 2024, Reykjavík District Court ruled in favor of Reykjavík municipality, finding that it had not significantly violated data protection laws in its use of the Seesaw platform. The Icelandic DPA appealed to the Court of Appeals also requesting to appeal the case directly to the Supreme Court.

## **Iceland's Data Protection Authority's inspection plan for 2023**

In February 2023, Persónuvernd published its inspection plan for 2023, focused on the following areas:

- Processing of personal data in smart solutions/software systems of financial institutions;
- Processing of personal data in smart solutions/software systems of insurance companies;
- Profiling and microtargeting;
- Processing of personal data in the field of fintech; and
- Processing of personal data in the field of healthtech.



# ? What are the most relevant **cybersecurity updates?**

## **Draft legislation for implementation of DORA**

In July 2024, draft legislation for the implementation of Regulation (EU) 2022/2554 of the European Parliament and of the council on digital operational resilience for the financial sector was introduced and opened for consultation. The scope of the draft legislation is extended from the regulation and also applies to pension funds in Iceland. It is estimated according to the draft legislation that the laws will come into effect in Iceland on 1 July 2025.

## **Implementation of NIS2 Directive**

On 1 November 2022, the first action plan for Icelandic authorities on cybersecurity was presented by the government. The action plan is based on Iceland's Cybersecurity Policy for the years 2022-2037, which was issued in February of the same year. Work is underway to implement the NIS2 Directive into Icelandic law.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## **Plans to amend Act No. 90/2018 on data protection and the processing of personal data**

The Icelandic Ministry of Justice has published plans and draft legislation to amend certain provisions of Act No. 90/2018 on Data Protection and the Processing of Personal Data and Act No. 75/2019 on the Processing of Personal Data for Law Enforcement Purposes. According to the ministry it has become apparent that several provisions need further clarification or amendment. The Ministry of Justice has also received suggestions that there is a reason to review the scope of the act in regards to the processing of personal data by the courts when exercising their judicial authority and various other provision e.g., on clearer definition of the term 'working documents' in Paragraph 4 of Article 17 of Act No. 90/2018 which are not subject to access requests from data subjects, clearer definition of the term 'security breach', and penalty provisions for violations of the confidentiality obligation of data protection officers.

## **Supreme Court hearing**

The Supreme Court of Iceland has agreed to hear the case brought by Reykjavík municipality against the Data Protection Authority, without it being reviewed by the Court of Appeal first. In the Supreme Court's decision, it is stated that the ruling in the case has general significance for the application of legal rules and the interpretation of laws on data protection and the processing of personal data, which were enacted in 2018. Furthermore, the ruling is of considerable precedent value as it is the first time that the Data Protection Authority's decision to impose administrative fines is being tested in court. Principal hearing is scheduled in October 2024.

## **Increased funding for the Icelandic Data Protection Authority**

There are plans to increase the funding for the Icelandic Data Protection Authority in order to enhance transparency and efficiency, public trust securing personal data processing in the business sector and by government authorities and to improve policymaking and planning, i.e., for proactive investigations and audits by the authority.

# Indonesia

## Contacts



**Cornel B. Juniarto**

Managing Partner, Deloitte Legal Indonesia  
[cbjuniarto@deloittelegal-id.com](mailto:cbjuniarto@deloittelegal-id.com)



**Stefanus Brian Audyanto**

Partner, Deloitte Legal Indonesia  
[saudyanto@deloittelegal-id.com](mailto:saudyanto@deloittelegal-id.com)

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

## **Issuance of Personal Data Protection Government Regulation draft to the public**

In August 2023, the Indonesian government through the Ministry of Communication and Informatics (MCI) issued the Government Regulation on Personal Data Protection draft (PDP GR Draft) to the public, as the main implementing regulation of Law 27 of 2022 on Personal Data Protection (PDP Law), which is Indonesia's main regulation governing personal data protection. The PDP GR Draft is expected to provide a technical guideline on personal data protection and will make way for further/detailed implementing regulations, including regulations which will be issued by the soon-to-be-established Indonesian Personal Data Protection Agency as the main regulating agency on personal data protection.

As of September 2024, the PDP GR Draft provide further governance on personal data protection, and comprises of several chapters, including:

- What constitutes as a personal data;
- Personal data processing provisions;
- Rights of data subject and obligations of data processor and/or data controller;
- Cross-border personal data transfer;
- International cooperations (*kerja sama internasional*);
- Establishment of Personal Data Protection Agency (*Lembaga Pelindungan Data Pribadi or Lembaga PDP*);
- Administrative sanctions; and
- Dispute settlement and procedural law.

Prior to its final enactment, the PDP GR Draft has undergone various steps and processes, including gaining public responses and comments. Such responses and comments have been followed-up with mapping, identification and analysis, as well as further discussion by the MCI and relevant stakeholders.

MCI have also conducted technical guidances (*bimbingan teknis*) to provide information on personal data protection and also evaluate the readiness of public officials (specifically relevant ministries and/or central agencies) handling personal data of the general public. In this respect, the existence of the National Data Center managed by MCI will become the mainstay in controlling and processing the personal data of citizens held by the government. Therefore, the success of the implementation of PDP Law will depend on (among others) the reliability of the National Data center in protecting the sovereignty of the managed citizens' data.

Throughout March to August 2024, representatives of relevant Ministries/Agencies have discussed and attended various discussion on the PDP GR Draft. On 23 August 2024, Inter-ministry Committee (*Panitia Antar Kementerian or PAK*) agree on several key points, including aligning of personal data protection and personal data processing norms and rights and obligations under the PDP GR Draft.

As of September 2024, the PDP GR Draft has been forwarded to the Indonesian Ministry of Law and Human Rights (MOLHR) for harmonization purposes. Upon completion of such harmonization, the PDP GR Draft will be finalized prior to its enactment thereafter. It is noteworthy that the government has yet issued official announcement/publication as to when the PDP GR Draft will be officially enacted, although it is expected for the PDP GR Draft to be enacted in 2024.





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

## **MCI Circular Letter on Artificial Intelligence Ethics**

The Indonesian government has few regulations governing Artificial Intelligence (AI), mainly through the MCI Regulation Number 3 of 2021 on Business Activity and Product Standards on Implementation of Risk-based Licensing in Post, Telecommunication and Electronic System and Transactions Sector (MCIR 3/2021). In relation to AI, MCIR 3/2021 governs on AI-based programming activities and defines the scope of such activity to AI-based programming activity covering consultation followed-up by analysis and programming via AI utilization, including subsets of AI such as machine learning, natural language processing, expert system and other AI subsets.

As one of the follow-ups of MCIR 3/2021, MCI has issued MCI Circular Letter Number 9 of 2023 on Artificial Intelligence Ethics (MCICL 9/2023). MCICL 9/2023 is issued to provide certain guidance and aims for AI technology is utilized in consideration of ethical, prudent and safety principles, and have positive impact orientation. Further, MCICL 9/2023 is also deemed necessary for effective implementation of AI, to minimize potential adverse impact of AI.

Further to its core aim, MCICL 9/2023 provides ethical guidance on:

- Formulation of internal company policies, implementation of public and private electronic system related to data and AI internal ethics; and
- AI-based consultation, analysis and programming in line with applicable laws and regulations.

MCICL 9/2023 governs that AI technology implementation shall consider the following principles (among others):

- Inclusivity;
- Humanity;
- Security;
- Accessibility;
- Transparency;
- Credibility and accountability;
- Personal data protection;
- Development and environmental continuity; and
- Intellectual property.

MCICL 9/2023 also provides additional governance related to the implementation of AI and responsibilities of relevant parties regarding such implementation of AI.



# What are the most relevant expected developments in **cybersecurity**?

## **National Cyber Security Action Plan for Year 2024-2028**

The Indonesian Cyber and Crypto Agency issued a regulation on the National Cyber Security Action Plan for Year 2024-2028, where the National Cyber Security Action Plan (National Action Plan) covers on several aspects, including:

- Policy direction;
- Challenges;
- Strategic goals;
- Activities;
- Success indicators;
- Target and annual goals;
- Stakeholders; and
- Relevant instances.

The National Action Plan governs on several focus areas, including governance, risk management, readiness and security, increase of vital information infrastructure protection, independence of national cryptographic, increase of capabilities, capacity and quality, cybersecurity policy, and international cooperation.

Each year (commencing as of 2024 up until 2028) has their own goals and target, and for each of the focus areas, the Indonesian Cyber and Crypto Agency is the main stakeholder responsible in the implementation of each aspects covered in the focus areas.

While there are various activities included in the focus areas, there are several key activities applicable, including (among others):

- Formulating the national cybersecurity standard and criteria;
- Coordinating in the formulation of electronic-based government system architecture;
- Setting cybersecurity risk profile on vital information infrastructure sectors
- Performing cybersecurity national risk assessment, etc.



# What are the most relevant expected developments in AI?

## Indonesia's Artificial Intelligence National Strategy (2020 – 2045)

In 2020, the Agency for the Assessment and Application of Technology (*Badan Pengkajian dan Penerapan Teknologi*, or BBPT) issued the Artificial Intelligence National Strategy for the years 2020-2025 (AI National Strategy). The AI National Strategy sets out certain points relating to AI, including strategic issues on AI ethics and policies and development of AI, as well as initiative programs related to AI.

The AI National Strategy document sets out high-level mapping for AI-related programs for the years 2020-2024, where in 2023-2024, the following program is expected to occur (among others):

- Establishment of AI policy supervision;
- Development of AI competence scheme;
- Development of national AI human resource talents;
- Development of integrated AI-based learning ecosystem;
- Ability of the nation/country to access all data required for its strategic interests; and
- Availability of AI machine learning infrastructure and platform, etc.

In continuation of the 2020-2024 program, the AI National Strategy document sets out high-level mapping for AI-related program from 2025-2045, covering various outputs and initiatives, including (among others):

- AI policy supervision by relevant ministries/agencies;
- Development of national AI human resource talents;
- Development of integrated AI-based learning ecosystem;
- Availability of AI machine learning infrastructure and platform;
- Availability of data connection system (between producers and consumers);
- Increase of national AI innovation system implementation; and
- Availability of AI-based products and services in various sectors, including administration and public information sector, health sector, education sector, public transportation sector, energy and utilities sector, financial and retail sector, etc.

However, it is unclear whether any additional laws and/or regulations will be enacted in the coming years in relation to AI development and/or utilization.

# Italy

## Contacts



**Ida Palombella**

Equity Partner, Deloitte Legal Italy  
[ipalombella@deloitte.it](mailto:ipalombella@deloitte.it)



**Pietro Boccaccini**

Director, Deloitte Legal Italy  
[pbocaccini@deloitte.it](mailto:pbocaccini@deloitte.it)



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

## 2023 Italian DPA annual report on personal data protection

In July 2024, the Italian Data Protection Authority (*the Garante per la protezione dei dati personali*) published its [annual report on personal data protection for the year 2023](#). The report summarizes the authority's key activities in 2023 across various sectors, such as public administration, healthcare, research activities, artificial intelligence, marketing, telemarketing, electronic communications, etc.

Some of the most relevant topics addressed by the authority have been digitalization and AI; additional areas include aggressive telemarketing, processing of personal data of vulnerable subjects and use of healthcare data.

The following numbers characterize the work done by the Italian DPA in 2023: (i) 634 board decisions; (ii) 9,281 complaints and reports managed; (iii) seven reports of facts to the criminal judicial authority; (iv) 394 corrective measures and sanctions issued; (v) almost €8 million collected from fines; (vi) 2,037 data breaches notified to the authority; and (vii) 144 inspections carried out.

Within the report, the Italian DPA has underlined the main obligations on organizations for the development and use of AI systems. Among such obligations, the authority underlined the relevance of assessing the risks and taking mitigation measures, verifying the training data set and the AI outcomes, storing the event logs for the entire system lifecycle and ensuring adequate transparency information, including in relation to the logic involved as well as the envisaged consequences of its use.

## Italian Data Protection Authority [Decision No. 12 of 11 January 2024](#)

### Code of conduct for the Employment Agencies

In January 2024, the Italian Data Protection Authority [approved the first code of conduct for Employment Agencies](#) (EA). This code of conduct, proposed by the Italian national association of employment agencies (Assolavoro), aims to regulate the processing of personal data in the screening, recruiting and selection of job candidates and employees.

The key aspects of the code of conduct can be summarized as follows:

- EAs are generally autonomous data controllers in relation to their activities, except when performing outsourcing services;
- EAs may process special categories of personal data only when necessary for specific and legitimate purposes related to employment, social security and social protection obligations and rights relevant to the contractual relationship with the employee or collaborator;
- EAs should generally collect personal data directly from the data subjects, however by ensuring adequate measures and procedures EAs may collect personal data from professional social networks;
- Data regarding candidates may be stored for a maximum of 48 months from the last activity carried out by the data subject (i.e., rolling) or up to 11 years from the termination of the employment contract in the case of staffing;
- Automated decision-making processes may be used in certain cases, subject to the consent of the data subject and the positive outcome of a DPIA (Data Protection Impact Assessment); and
- EAs may not collect references from former employers and communicate them to their clients without a prior authorization from the job applicant.

## The Italian Data Protection Authority's opinion on the processing of email metadata in the workplace

With a controversial decision, which prompted the decision to carry out a public consultation, [the Italian Data Protection Authority provided some guidelines on how metadata should be processed by the employers in the workplace](#).

Following the public consultation, the Italian Data Protection Authority issued an updated version of such guidelines with the Decision No. 364 of 6 June 2024.

The guidelines clarify that the metadata in question are the logs generated by interactions between the mail transport agent (MTA) servers and workstations during communication between servers and, if applicable, clients. This metadata includes:

- The email addresses of the sender and recipient;
- IP addresses of the server or clients involved in the message routing;
- Times of the sending, retransmission or reception;
- Size of the message and dimension of any attachment; and
- Subject of the sent or received message.

The new guidelines state that employers can retain the metadata of employees' emails only if necessary for the functioning of the email system's infrastructure and only for up to 21 days.

A longer retention period is permissible only if special circumstances apply, in consideration of the specific organizational and technical characteristics of the company. These circumstances must be demonstrated by the data controller in accordance with the GDPR's principle of accountability.

In such cases, the employer must implement appropriate technical and organizational security measures, including to ensure that:

- The metadata are not processed for other purposes;
- Access to the metadata is restricted to authorized and appropriately trained personnel; and
- Logs are kept to track access.

If metadata is retained for more than 21 days the data controller must comply with Article 4 of the Worker's Statute, by either:

- Reaching an agreement with the trade unions, or
- Obtaining an authorization by the Labour Inspectorate.

If compliance with these rules is not possible, the use of the programs and services must cease immediately.

The authority also provided recommendations for employers to ensure compliance with the data protection obligations, including:

- Conducting a Data Protection Impact Assessment (DPIA);
- Documenting a Legitimate Interest Assessment (LIA);
- Ensuring that all data processing agreements with relevant data processors are executed in compliance with the applicable requirements; and
- Properly informing employees of the types of processing operations carried out on their data, including by providing appropriate information in policies.

## Legislative decree harmonizing the Italian legal framework to the Data Governance Act

On 10 October 2024, [the Legislative Decree No. 144 aligning the Italian legal system to the Data Governance Act](#) (EU Regulation 2022/868) (DGA) has been published in the Official Gazette.

The legislative decree designates the Agenzia per l'Italia Digitale - Agency for Digital Italy (AgID) as the competent authority for:

- The single information point pursuant to Article 8 of the DGA;
- The notification by data intermediation services providers;
- The registration of data altruism organizations; and
- The monitoring and control function to ensure that "data intermediation service providers" and "data altruism organizations" comply with the obligations and requirements set out in the DGA.

The decree strongly underlines the close cooperation that needs to take place between AgID, the National Cybersecurity Agency (ACN), the Competition Authority (AGCM), and the Italian Data Protection Authority (Garante), also providing that non-binding cooperation agreements may be entered into among such parties.

For the infringements of the obligations provided in the DGA, AgID may adopt administrative pecuniary sanctions ranging from a minimum of €10,000 to a maximum of €100,000, or, for companies, up to 6% of the total worldwide annual turnover of the previous financial year.

## New data protection training materials for small and medium enterprises

In the context of the ARC project (Awareness Raising Campaigns, supported by the EU Commission) and in partnership with the Italian Data Protection Authority, [useful training materials have been made available to support small and medium enterprises](#) in raising the awareness of their employees in relation to the data protection area.

The training programme consists of 15 modules and includes some useful tools, such as a model to carry out a data protection impact assessment and a legitimate interest assessment.

Olivia is free of charge and is available also in English.

## The Garante sanctions an energy company due to shortcomings in their security protocols in relation to marketing activities

Following a thorough investigation, the Italian Data Protection Authority sanctioned an energy company for inadequate security measures in their marketing and telemarketing activities conducted by their sales network.

The authority found that the company had failed to implement appropriate security measures in relation to the access to their systems; appropriate measures would have had to ensure the correct use of access credentials and prevent the sharing of credentials. The Garante noted that it was too easy for external sales companies to have access to the system and upload contracts, even without having a contract with the energy company.

As a result of such infringements, the authority imposed the highest sanction ever issued by the Garante up to such date.

# ? What are the most relevant **cybersecurity updates?**

## Legislative decree implementing the NIS2 Directive

On 1 October 2024, [the Legislative Decree No. 138/2024 implementing the NIS2 Directive](#) was published on the Official Journal of the Italian Republic. The legislative decree:

- Confirms the National Agency for Cybersecurity (Agenzia per la Cybersicurezza Nazionale - ACN) as:
  - The National authority competent for the NIS legal framework;
  - The NIS single point of contact;
  - The authority within which Computer Security Incident Response Team (CSIRT Italia) is constituted at national level;
- Provides that entities falling within the scope must register (or update) their position every year between the 1 January and 28 February, while by the 31 March, the ACN will draw up the list of the entities falling within the scope on the basis of the communications received and will notify to the registered entities the inclusion, permanence or removal from the list; to carry out such activities, entities shall assess if they fall within the scope of such legislation as soon as possible;
- Provides that from the 15 April to 31 May each year, the subjects who have received the communication will provide further information through the digital platform made available by the ACN;
- Designates the CSIRT Italy as coordinator for the purpose of vulnerability disclosure and clarifies its tasks; and
- Defines the security risk management measures and the incident reporting obligations and sets forth the security measures and data governance obligations provided by the directive, including the obligation to ensure the security of the supply chain.

## Legislative decree implementing the CER Directive

With [Legislative Decree No. 134/2024](#), the Critical Entities Resilience (CER) Directive ([No. 2022/2557](#)) was officially implemented in Italy.

The directive and the implementing legislative decree aim to ensure the provision of essential services in the internal market, enhance the resilience of critical entities and improve cross-border cooperation between competent authorities. The legislative decree establishes:

- The creation of a Single Point of Contact (PCU – *punto di contatto unico*) for the cyber resilience of critical entities within the Presidency of the Council of Ministers with various coordination and support functions;
- The identification of Sectorial Competent Authorities (ASC – *autorità settoriali competenti*), which must designate “critical entities” for each sector and sub-sector by the 17 of January 2026, and communicate such subjects to the Single Point of Contact;
- The criteria for identifying critical entities of particular European significance (SCRE – *soggetti critici di particolare rilevanza europea*);
- The creation of an Inter-ministerial Committee for Resilience (CIR – *comitato interministeriali per la resilienza*) within the Presidency of the Council of Ministers;
- The requirement for critical entities to adopt technical and organizational security measures to ensure their resilience; and
- The obligation for critical entities to submit a notification of relevant incidents without undue delay to the competent authority and to the Single Point of Contact no later than 24 hours after becoming aware of it.

This legislation should be read in conjunction with the NIS2 legal framework.



## New Cybersecurity Act

In July 2024, the new law on cybersecurity ([Law No. 90/2024](#)) officially entered into force.

The act has the aim to improve Italy's efficiency regarding the cybersecurity of the state and to do so, new measures have been proposed:

- Implementation of new security protocols for the protection of national critical infrastructures against cyberattacks;
- Prevention and suppression of cybercrimes through the introduction of new types of criminal offences and the toughening of existing ones, with particular focus on crimes against electronic communications; and
- Promotion of agreements and collaborations with other states to improve the global response to cyberthreats.

The law provides for an obligation to notify the Agency for National Cybersecurity (ACN) on all cybersecurity major incidents without undue delay and within 24 hours, providing the complete information within 72 hours.

The law also requires the subjects within its scope to identify an IT department responsible to ensure the implementation of cybersecurity measures as well as a cybersecurity manager, to be communicated to ACN.

The second part of the law amends the Italian Criminal Code and the Italian Code of Criminal Procedure to expand the scope of application and/or toughen the sanctions and legal procedures of some criminal offences.

This new cybersecurity act complements and shall be read with a cross-cutting approach by taking into consideration the complete EU cybersecurity legal framework, such as also the NIS2 and the CER directives.

## ACN Incident Notification Guide to CSIRT Italy

In July 2024, the National Cybersecurity Agency (ACN), [published guidelines on how to notify possible incidents to the CSIRT](#) (Computer Security Incident Response Team).

The guidelines provide a comprehensive set of instructions for various entities, such as: (i) public and private entities required by law to notify incidents; (ii) subjects included in the National Cybersecurity Perimeter; and (iii) telecommunication providers and entities covered by Law No. 90/2024 on strengthening national cybersecurity and combating cybercrimes.

The incident notification to the CSIRT Italy is divided into four phases:

- Preparatory phase: The reporting subject gathers all the minimum information to perform the notification with the aim of permitting to the authority a sufficient knowledge of the event;
- Incident reporting phase: The reporting subject must complete a form available on the CSIRT Italy website. The notification shall be submitted within the deadline provided by law;
- Management of the notification: This phase involves the “incident handling” operations by the CSIRT to support the affected entity through response and recovery actions; and
- Closure phase: Once the support activities in handling the incident are completed (possibly also planning future recovery phases) the CSIRT will close the incident.

## Cyber threats in the health sector – the ACN Report from 2022 to 2024

In a [report published in September 2024](#), the National Agency for Cybersecurity (ACN) pointed out that the health sector is primary target of cyberattacks, which surged by a staggering 50% from 2022 to 2023. These attacks significantly threaten the privacy of patient's data, as well as the overall well-functioning of health services.

The ACN's analysis attributes this rise to poorly managed or entirely neglected security practices. To address this, the ACN has therefore issued several recommendations for healthcare facilities, such as: (i) implementing a multi-factor authentication; (ii) adopting a password policy and a backup policy; (iii) setting up an incident response plan; and (iv) establishing a log management policy.

Additionally, with the recent adoption of the NIS2 Directive, the healthcare sector has been included in the category of subjects considered important or essential, bringing several new obligations, such as:

- Monitoring incident management measures implemented by relevant bodies;
- Adopting adequate and proportionate measures to address potential cyber risks;
- Conducting security checks on the supply chain; and
- Notifying the competent authority of relevant incidents within 24 hours from the discovery.

## Guidelines on the storing of passwords

In December 2023, the National Agency for Cybersecurity (ACN), in collaboration with the Italian Data Protection Authority, [issued specific guidelines on the storing of passwords](#), often a root cause of personal data breaches.

The guidelines aim is to provide recommendations on the cryptographic functions currently considered most secure for password storage, to prevent authentication credentials (username and password) from being compromised and falling into the hands of cybercriminals, to then be published online (particularly, on the dark web) or used for identity theft, ransom demands or other types of attacks.

The guidelines are addressed to all private and public entities which store user passwords on their systems, particularly when such credentials are necessary to access data relating to a large number of data subjects, database of significant dimension or sensitivity, or are used by entities that typically process judicial data or personal data relating to special categories (e.g., lawyers, doctors).

In summary, the guidelines:

- Recommend the use of robust cryptographic functions, providing instructions and recommendations on the functions currently considered to be most "secure";
- Emphasize the need of password hashing, explaining in detail the commonly used algorithms; and
- Offer guidance on the most recommended algorithms and the respective parameters.

The guidelines also stress that controllers and processors of the systems should not store the passwords for longer than necessary to verify the user identity and to permit the access to the information systems or online services.



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

## Draft national AI law complementing the EU AI Act

A [draft law introducing new regulations to address the misuse of Artificial Intelligence, complementing the EU AI Act](#), is currently awaiting parliamentary approval.

The proposed law aims to promote a fair, transparent and responsible use of AI, reaffirming the principles (enshrined in the EU AI Act) that should guide its development and use.

In addition, the draft law includes provisions specific to certain sectors, such as:

- AI use in healthcare and disability sectors must not select or condition access to health care services based on discriminatory criteria;
- AI must not discriminate against employees in consideration of gender, age, personal, social or economic conditions etc.;
- Intellectual professionals must inform their clients about the use of AI;
- Public administrations may use the AI to enhance the efficiency of administrative activities and improve the quality and quantity of services for citizens and companies; and
- In the administration of justice, AI systems may only be used for instrumental and support purposes and the interpretation of law shall always be performed by a judge;

Eventually, the draft law designates the Agency for a Digital Italy (AgID) and the National Agency for cybersecurity (ACN) as the national authorities responsible for AI compliance obligations.

On 2 August 2024, the Italian Data Protection Authority provided its opinion on such draft law recommending several amendments.

## Guidance of the Italian DPA on the measures to defend personal data published online from the web scraping practice

Following a fact-finding investigation that began in late 2023, in May 2024 the [Italian DPA issued guidance on how to protect personal data published online from web scraping](#), i.e., the indiscriminate collection of personal data on the internet, carried out by third parties for the purpose of training Generative AI models.

The authority's recommended measures include:

- Creating reserved areas, accessible only by prior registration, to conceal data from the public;
- Including anti-scraping clauses in the terms and condition of websites;
- Monitoring the internet traffic from web pages to identify possible anomalies in the flows of incoming or outgoing data; and
- Implementing specific measures against bots using technological solutions provided by the same companies responsible for web scraping.

The authority specified that, although such measures are not mandatory, the data controllers should evaluate, in accordance with the principle of accountability, whether to adopt such measures to prevent or mitigate the effects of web scraping, considering the state-of-the-art technology and the implementation costs.

## **G7 Data Privacy Authorities – the role of AI with regards to children, data circulation and international cooperation**

In October 2024, the G7 Data Privacy Authorities (DPAs) convened in Rome to discuss their enforcement practices and priorities. At the forefront of the discussions was attention to ethical and trustworthy development of AI, children's privacy, geolocation data, health privacy, security and online advertising.

The authorities agreed on the importance of adopting adequate safeguards for minors in the development and use of artificial intelligence. On this topic, two key documents were issued (i) a statement emphasizing the crucial role of DPAs in fostering trustworthy AI (underscoring their experience and independence as crucial in addressing such a sensitive matter); and (ii) a "Statement on AI and Children" calling for urgent measures to protect children's privacy.

The G7 DPAs also released a communiqué, which stressed the importance of robust cross-border data transfer mechanisms that safeguard personal data, enabling secure and free data flows.

In a significant step forward, the G7 DPAs endorsed an action plan for 2024-2025, centered on three main pillars:

- Developing Data Free Flow with Trust (DFFT), to strengthen transfer tools;
- Studying the implications of emerging technologies, with a focus on collaboration in personal data protection and strategic support; and
- Reinforcing enforcement cooperation, enhancing dialogue amongst G7 DPAs and the broader data protection and privacy enforcement community.

## **The Garante fines a municipality for making use of AI systems of surveillance for scientific research**

The Garante became aware through news reports that an Italian municipality had deployed AI systems in public areas to collect data by video-cameras and microphones, aiming to prevent potential situations of public danger, such as urban security issues, hate crimes and terror attacks.

After an extensive investigation, the authority found that the measures implemented by the controller, such as the alleged anonymization of the personal data collected, were not inadequate.

Furthermore, the DPA found the breach of the principle of lawfulness. The laws that the controller cited as the applicable legal basis for the processing were deemed a not valid legal ground, considering that the law itself should provide specific rules on the scope and limits of the processing operations.

The Garante also held that the controller failed to: (i) properly provide information about the processing operations; and (ii) conduct a proper Data Protection Impact Assessment (the document lacked the date of approval and the signature of a representative of the municipality, and did not cover all the relevant processing operations). Ultimately, the DPA considered that, given the intrusiveness of the processing operations on the rights and freedoms of the data subjects, the municipality should have sought the opinion of the citizens on the initiative.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## ACN guidelines on the implementation of the NIS2 obligations

In accordance with the legislative decree implementing the NIS2 Directive, it can be expected that the ACN will publish guidelines and recommendations in connection with the NIS2 legal framework.

## The inspections of the Data Protection Authority – inspection plan for the second semester of 2024

In its decision dated 4 July 2024, the Italian Data Protection Authority has published its [inspection plan for the second semester of 2024](#), deciding to focus on:

- Companies specializing in commercial information and creditworthiness assessments;
- Data processing activities carried out for telemarketing purposes;
- The activation of unsolicited contracts in the energy sector;
- Data processing carried out in the context of connected vehicles;
- Use of cookies by major digital service providers;
- Companies that manage alarm systems with remote audio/video connection capabilities;
- Trust services providers of digital identity and their supply chain;
- Use of “electronic register platforms and digital suites” by schools; and
- Other facts submitted to the authority with formal complaints and reports.

Further to the inspections of the Garante, it is expected that there will be decisions on the abovementioned areas during 2025.

## Pay or consent cookie wall

The Italian Data Protection Authority lately has carried out various investigations in relation to the use of cookie walls.

The authority might adopt some decisions in relation to such practices in the upcoming months.

## Garante guidelines on video-surveillance

The Italian Data Protection Authority is expected to issue new guidelines on the use of video surveillance.

This guidance will update the 2010 decision relating to the use of CCTV systems.

## Investigations in relation to GenAI and AI systems trainings

The Italian DPA has carried out various investigations in relation to the processing of personal data by AI systems, including Generative AI models.

Therefore, it can be expected that decisions will be issued in 2025 on certain cases relating (i) to the training of AI systems involving personal data, (ii) to web scraping practices, and (iii) to the use of GenAI technologies by editors online.

# Côte d'Ivoire

## Contacts



**Ursula Dutauziet**

Partner, Deloitte Côte d'Ivoire  
[udutauziet@deloitte.fr](mailto:udutauziet@deloitte.fr)



**Audrey Allo-Ello**

Manager, Deloitte Côte d'Ivoire  
[nallo-ello@deloitte.fr](mailto:nallo-ello@deloitte.fr)

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

- ARTCI [Decision No. 2024-1134](#) warning and formal notice to Moov Africa Côte d'Ivoire regarding the protection of personal data (18 September 2024).
- [Decision No. 2024-1095](#) of the ARTCI authorizing the processing of personal data by Pro Logistics “video surveillance” (on-board cameras) (24 July 2024).
- ARTCI [Decision No. 2024-1092](#) authorizing Consultech to process personal data (24 July 2024).
- ARTCI [Decision No. 2024-1091](#) authorizing BMI-WFS (World Financial Services) to process personal data (24 July 2024).
- ARTCI [Decision No. 2024-1090](#) authorizing Goodwill Audit & Consulting to process personal data (24 July 2024).
- [Decision No. 2024-1089](#) of the ARTCI authorizing the processing of personal data by Galance Group (24 July 2024).
- ARTCI [Decision No. 2024-1088](#) authorizing the transfer of personal data to the United States by Tolbi (Amazon Web Services) (24 July 2024).
- ARTCI [Decision No. 2024-1087](#) authorizing the processing of personal data by Tolbi (parcels georeferencing) (24 July 2024).
- ARTCI [Decision No. 2024-1086](#) authorizing Synergie Integrale to process personal data (24 July 2024).
- ARTCI [Decision No. 2024-1085](#) authorizing the processing of personal data by Tolbi (compliance with international standards) (24 July 2024).
- [Decision No. 2024-1084](#) of the ARTCI regulatory council authorizing the processing of personal data by Tolbi (sustainable development, improving producers' incomes) (24 July 2024).
- [Decision No. 2024-1083](#) of the ARTCI authorizing the processing of personal data by Proline Logistics “video surveillance” (24 July 2024).
- [Decision No. 2024-1079](#) of the regulatory board of the Côte d'Ivoire telecommunications/ICT regulatory authority, dated 18 July 2024, authorizing the processing of personal data by Simbrella.
- [Decision No. 2024-1078](#) of the ARTCI authorizing the processing of personal data by Atlantic Assurance Vie Côte d'Ivoire (AAVIE-CI) (18 July 2024).
- [Decision No. 2024-1076](#) of the ARTCI authorizing the processing of personal data by Atlantic Business International (ABI) (18 July 2024).
- [Decision No. 2024-1072](#) of the ARTCI authorizing the processing of personal data by Tridem Pharma Afrique Francophone (video surveillance of the headquarters) (18 July 2024).
- ARTCI [Decision No. 2024-1069](#) authorizing the transfer of personal data to France by Emailing Management (Mailjet) (18 July 2024).
- ARTCI [Decision No. 2024-1068](#) authorizing the processing of personal data by Emailing Management (18 July 2024).

- [Decision No. 2024-1067](#) of the ARTCI authorizing the processing of personal data by the Label company (18 July 2024).
- ARTCI [Decision No. 2024-1057](#) authorizing the processing of personal data by Le Terminal de San Pedro (TSP) (27 May 2024).
- ARTCI [Decision No. 2024-1056](#) authorizing the transfer of personal data to the United States by Fleetit (SquareGPS) (27 May 2024).
- ARTCI [Decision No. 2024-1055](#) authorizing the transfer of personal data to the United States by Fleetit (Microsoft Corporation) (27 May 2024).
- [Decision No. 2024-1054](#) of the ARTCI authorizing the processing of personal data by Fleetit (Geolocation) (27 May 2024).
- [Decision No. 2024-1053](#) of the ARTCI authorizing the processing of personal data by Fleetit (fleet management) (27 May 2024).
- [Decision No. 2024-1039](#) of the ARTCI authorizing the processing of personal data to the United States by Neris (Billetic.net order management) (24 May 2024).
- [Decision No. 2024-1038](#) of the ARTCI authorizing the processing of personal data by Neris (Billetic.net order management) (24 May 2024).
- [Decision No. 2024-1037](#) of the ARTCI authorizing the processing of personal data by Neris (Billetic.net order management) (24 May 2024).
- ARTCI [Decision No. 2024-1010](#) authorizing the processing of personal data by the insurance companies' association (25 January 2024).



# ? What are the most relevant **cybersecurity updates?**

The NIS2 directive does not apply to African countries, notably Côte d'Ivoire.

In Côte d'Ivoire, the Ministry of the Digital Economy, Telecommunications and Innovation has adopted the “National Cybersecurity Strategy 2021-2025”.

The strategic and specific objectives of this guideline are as follows:

- Strengthen the legal framework;
- Protect cyberspace;
- Strengthen digital trust; and
- Overhaul the institutional framework.



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

Apart from the UNESCO “Recommendation on the Ethics of Artificial Intelligence” adopted in November 2021, Ivorian legislation does not provide a legal framework governing artificial intelligence.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Data Protection

**The Telecommunications Regulatory Authority of Côte d'Ivoire (ARTCI) perspectives for the next 12 months are as follows:**

- Organization of the hackathon and the international conference as part of the celebration of 10 years of personal data protection;
- Commissioning of the certification platform for applicants for approval;
- Finalization of the study on advanced technologies;
- Online monitoring of websites;
- Continuation of the compliance process for private companies, public administrations, and institutions of the republic;
- Continuation of the 2023 monitoring program and preparation of the annual program for the 2024 fiscal year; and
- Establishment of a procedure for handling complaints and claims related to personal data protection.

## Cybersecurity

The Ministry of Telecommunications and Innovation's "National Cybersecurity Strategy 2021-2025".

## Artificial intelligence

On 30 September 2024, Côte d'Ivoire took a new step towards digital modernization with the launch of work to develop the National Strategy for Artificial Intelligence and Data Management. The National AI and Data Management Strategy of Côte d'Ivoire marks the beginning of a new technological era for the country, positioning it as a key player in the adoption of artificial intelligence in Africa.

# Japan

## Contacts



**Norikazu Otaki**

Managing Director, Deloitte Legal Japan

[norikazu.otaki@tohmatu.co.jp](mailto:norikazu.otaki@tohmatu.co.jp)



**Satoshi Yoshida**

Attorney-at-law, Deloitte Legal Japan

[satoshi6.yoshida@tohmatu.co.jp](mailto:satoshi6.yoshida@tohmatu.co.jp)



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

## **Amendment to the Enforcement Rules for the Act on the Protection of Personal Information to expand the scope of data breach notification requirements**

The Amendment to [the Enforcement Rule \(the Enforcement Rule\) for the Act on the Protection of Personal Information \(the Act\)](#), which was promulgated on 27 December 2023, came into effect on 1 April 2024. This amendment expands the scope of data breach notification requirements under the Act.

Article 26(1) of the Act delegates to the Enforcement Rule the task of defining the triggering events for data breach notifications. Prior to this amendment, the scope of the requirement to report to the Personal Information Protection Commission and to notify identifiable persons in the event of a potential leak for fraudulent purposes, etc., was limited to “personal data”, which is “personal information” that constitutes a “personal information database, etc.”. Due to this limitation, a leak of personal information that did not yet constitute a personal information database (e.g., web skimming attacks) was outside of the scope.

To address this issue, this amendment expands the scope to include “personal information” that is intended to be treated as “personal data”.

In accordance with this amendment, the "[Guidelines on the Act on the Protection of Personal Information \(General Provisions\)](#)" was also revised in December 2023.

## **Personal Information Protection Committee issued an alert regarding the use of cloud services**

Under the [Act on the Protection of Personal Information](#), when a business operator handling personal information uses a cloud service, even if the electronic data stored on that cloud

service contains personal data, if the cloud service provider “is not supposed to handle the personal data in question”, it is not considered to have provided the personal data to the cloud service provider, so there is no need to obtain the individual's consent, which is required by Article 27(1), or obligation to supervise the cloud service provider, which is required by Article 27(5)(i). In addition, the cloud service provider does not fall under the category of a business handling personal information.

However, on 25 March 2024, the Personal Information Protection Commission issued [administrative guidance](#) to a cloud service provider, finding that they had been handling personal data and that their safety management measures were inadequate.

The commission considered that the cause of this incident was a lack of understanding of the law, and on the same day issued “[Points to Keep in Mind \(Alert\) When a Cloud Service Provider Falls Under the Personal Information Protection Act's Definition of a Business Handling Personal Information](#)”.

In the alert, the commission clarified that the following circumstances were factors to be considered in the above incident.

- The terms of service stated that the cloud service provider could use the personal data of cloud service users in certain cases;
- The cloud service provider held a maintenance ID and was able to access the personal data of cloud service users, and no technical access control measures were in place to prevent handling; and
- The cloud service provider actually handled the personal data of cloud service users after exchanging a confirmation document with them.



## Amendments to Unfair Competition Prevention Act to expand the scope of protecting big data

[The Unfair Competition Prevention Act](#) (the Act), [amended in 2023](#) to expand the scope of protecting big data, came into effect in 2024.

The Act defines actions and behaviors that involve unlawful use of the results of technical development, product development, or other accomplishments achieved by someone else, as unfair competition.

The amendments to the Act in 2018 defined valuable data satisfying specific requirements (such as big data) as “[Shared Data with Limited Access](#)” and unauthorized acquisition/use, etc. as unfair competition actions, and set forth remedies such as claim for injunction against such actions. The “[Guidelines on Shared Data with Limited Access](#)”, originally published in 2019, presents a definition of shared data with limited access, requirements that fall under unfair competition, and other relevant matters.

When the Act was amended in 2018, it was assumed that big data that was to be shared with other parties would not be confidentially managed, so the Act in 2018 only protected “big data that is not confidentially managed”. However, in recent years, there have been cases of companies providing others with big data that is under confidential management within their own company, so the amendments to the Act in 2023 expands the scope to include “big data under confidential management”, allowing for integrated management of trade secrets and other information.

Reflecting these amendments, the Guidelines on Shared Data with Limited Access was also [revised in 2024](#).

## Amendments to Next Generation Medical Infrastructure Act, creating a new category of data called “pseudonymized medical data”

[The Act on Anonymized Medical Data That Are Meant to Contribute to Research and Development in the Medical Field](#) (commonly known as the Next-Generation Medical Infrastructure Act), which originally came into effect in 2018, promotes the use of “anonymized medical data” (such as health checkup results and medical records) in medical research and development.

In addition to “anonymized medical data”, [the amendments to the act in 2023](#), which came into effect in 2024, established a new system for creating and providing “pseudonymized medical data”. (The name of the act was also changed to the Act on Anonymized Medical Data and Pseudonymized Medical Data That Are Meant to Contribute to Research and Development in the Medical Field.)

“Pseudonymized medical data” refers to data that has been processed so that individuals cannot be identified unless it is cross-checked with other information. Although it is necessary to delete names and IDs, etc. from personal information, it is not necessary to delete unique values or rare disease names, etc. unlike “anonymized medical data”.

From the perspective of protecting personal information, “pseudonymized medical data” is only provided to users approved by the government.

The amendments to the act in 2023 also enabled the linkage analysis of “anonymized medical data” and public databases such as the National Database of Health Insurance Claims (NDB) and the Japanese Long-term Care Database.

# ? What are the most relevant **cybersecurity updates?**

## The Economic Security Promotion Act

The Economic Security Promotion Act ([Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures](#)) was enacted in 2022, and the [part for introducing systems for ensuring stable provision of essential infrastructure services](#) came into effect in May 2024.

Under this act, specified essential infrastructure service providers must notify the competent minister the plan related to installation and entrustment of maintenance, etc. of critical facilities for the minister's screening (whether or not critical facilities are at high risk of being misused as a means for actions to disrupt stable provision of services from outside Japan).

This requires various risk management measures, such as ensuring cybersecurity.

## The Act on the Protection and Utilization of Critical Economic Security Information

In May 2024, [the Act on the Protection and Utilization of Critical Economic Security Information](#) was enacted and came into effect.

Under this act, certain information concerning critical economic foundation (critical infrastructure and supply chains of products), which is not publicly disclosed and particularly required to be kept secret due to the risk of causing damage to the national security, if disclosed without authorization (e.g., information related to cyberthreats and countermeasures and information related to vulnerabilities in the supply chain) is designated as "critical economic security information."

The duty of handling critical economic security information is restricted to those who have been found to have no risk of unauthorized disclosure of critical economic security information in the security clearance assessment.

## Cybersecurity-related Laws and Regulations Q&A Handbook Ver. 2.0

In September 2023, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) released the revised version of the "[Cybersecurity-related Laws and Regulations Q&A Handbook](#)" for the first time since its initial version in 2020 (only Japanese version).

This book explains in the clearest possible terms the legal issues associated with peacetime cybersecurity measures and corporate incident response, as well as the legal issues arising from changes in laws and regulations regarding information handling and other matters.

This version 2.0 includes a number of new Q&A topics, including:

- Response to authorities during a cybersecurity incident;
- Drones and cybersecurity;
- Regulations in critical infrastructure sectors;
- Mobility and cybersecurity;
- DX Certification/DX Stocks and cybersecurity;
- Standards related to cybersecurity and the NIST SP800 series;
- Laws and regulations related to authentication/identity verification; and
- Response to ransomware.



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

## AI Guidelines for Business Ver1.0

### Background

In April 2024, the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) released "[AI Guidelines for Business Ver1.0](#)".

The guidelines present unified guiding principles in AI governance in Japan to promote safe and secure use of AI. It is intended to help people who use AI in various businesses to fully recognize AI risks based on international trends and stakeholders' concerns, and to voluntarily take the necessary countermeasures across the entire lifecycle.

The guidelines aim to actively and cooperatively develop a framework that achieves both promotion of innovation and reduction of risks across the lifecycle through mutual cooperation among interested parties in implementing the common guiding principles, important matters for each AI business actor, and AI governance.

### Targets

The guidelines are intended for all AI business actors (including public institutions such as governments and municipalities) who develop, provide, or use AI in various businesses.

- AI developer: Business operators who develop AI systems (including business operators who research AI).
- AI provider: Business operators who incorporate AI systems into applications, products, or existing systems, business processes, etc., and provide them to AI business users and, in some cases, non-business users as services.
- AI business user: Business operators who use AI systems or AI services in their businesses.

### Structure

The guidelines consist of [the main part and the appendix](#). The main part covers "the efforts to be made regarding AI (guiding principles = what)" based on "the ideal society while considering stakeholders' expectations (basic philosophies = why)" that are important for using AI safely and securely to maximize the benefits of AI.

The appendix covers "the specific approach to be adopted (implementation = how)" to lead AI business actors to take actual implementation of the principles. The descriptions in the appendix correspond to those in the main part and serve as a supporting document for the reading of the main part and considerations and actions based on the main part.

	Main part (why, what)	Appendix (how)
For all AI business actors	Part 1 Definitions	1. Relevant to Part 1 [About AI] A. Preconditions for AI B. AI's benefits and risks
	Part 2 Society to aim for with AI, and matters each AI business actor works on A. Basic philosophies B. Principles C. Common Guiding Principles for AI business actors involved in advanced AI systems D. Common Guiding Principles for AI business actors involved in advanced AI systems E. Building AI governance	2. Relevant to Part 2 [E.Building AI Governance] A. Building of AI governance and monitoring by management B. Examples of business operator's efforts at AI governance
	Part 3 Matters Related to AI Developers * Includes additional matters described in "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems" as well	3. Relevant to Part 3 [For AI Developers] A. Descriptions of Part 3 "Matters Related to AI Developers" B. Descriptions of "Common Guiding Principles" in Part 2 C. Matters to be observed in developing advanced AI systems
For each AI business actor	Part 4 Matters Related to AI Providers	4. Relevant to Part 4 [For AI Providers] A. Descriptions of Part 4 "Matters Related to AI Providers" B. Descriptions of "Common guiding principles" in Part 2
	Part 5 Matters Related to AI Business Users	5. Relevant to Part 5 [For AI Business users] A. Descriptions of Part 5 "Matters Related to AI Business Users" B. Descriptions of "Common Guiding Principles" in Part 2
Other references		6. Major precautions for referring to "Contract Guidelines on Utilization of AI and Data" 7. Checklist 8. Cross-actor virtual cases 9. References for overseas guidelines, etc. The appendices 7, 8, and 9 are Japanese only.





## Advisory Panel for the Agency for Cultural Affairs published “General Understanding on AI and Copyright”

In March 2024, “[General Understanding on AI and Copyright](#)” was published by an advisory panel for the Commissioner of the Agency for Cultural Affairs. The panel, consisting law scholars, lawyers, judges and other experts with knowledge of copyright laws and other intellectual property laws, discussed how the current Copyright Act should be applied in relation to AI, aiming to provide a general understanding of this topic.

They discussed over three main topics:

- Exploitation of copyrighted works for AI development/training etc.;
- Copyright infringement in the generation and utilization of AI-generated materials; and
- Criteria for determining the copyrightability of AI-generated material.

### AI development/training stage

Article 30(4) of the Copyright Act may allow the exploitation of copyrighted works not for enjoyment of the thoughts or sentiments expressed in the copyrighted work (exploitation for non-enjoyment purposes) such as AI development or other forms of data usage, without the permission of the copyright holder.

In this context, “Enjoyment” refers to obtaining the benefit of having the viewer’s intellectual and emotional needs satisfied through using the copyrighted work.

Article 30(4) of the Copyright Act does not apply in cases where it would unreasonably prejudice the interests of the copyright holder.

The main issues discussed in connection with Article 30(4) are (i) cases not meeting the “non-enjoyment purpose” requirement, and (ii) cases that would unreasonably prejudice the interests of the copyright holder.

### Generation/utilization stage

Requirements to constitute copyright infringement:

- When AI-generated images or copies thereof are uploaded to social media or sold, copyright infringement will be determined based on the same criteria as for traditional infringement cases.
- In other words, if an AI-generated image or any other creation is found to have similarity (i.e., common creative expression) and dependency (i.e., creation based on an existing copyrighted work) with an existing image or copyrighted work, and there are no applicable copyright exceptions, it will be considered an infringement of copyright.

The main issues discussed in relation to the concept of copyright infringement are:

- “Dependency” in the context of AI-generated work;
- Countermeasures for addressing copyright infringement; and
- Cases in which AI-related businesses may be liable for copyright infringement.

### Copyrightability of AI-generated material

According to the Copyright Act, a (copyrighted) “work” is defined as a “creatively produced expression of thoughts or sentiments that falls within the literary, academic, artistic, or musical domain.”

Materials autonomously generated by AI are not considered “creatively produced expressions of thoughts or sentiments” and therefore are not classified as (copyrighted) “works.”

On the other hand, if AI is used as a “tool” by a person to creatively express thoughts or sentiments, such material is considered a “work”, and the user of the AI is regarded as the “author”.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Amendments to Act on the Protection of Personal Information based on “Every-Three-Year Review” process

When [the Act on the Protection of Personal Information](#) was revised in 2020, it was decided that it would be reviewed every three years.

In November 2023, the Personal Information Protection Commission began considering the three-year review, and in February 2024, it announced [the following draft items for consideration in the three-year review](#).

- How to more substantially protect the rights and interests of individuals, including:
  - Rules on the proper handling of personal information, etc. (proper acquisition, improper use, personal information, biometric data, etc.);
  - Restrictions on providing information to third parties (opt-out, etc.);
  - Rules regarding personal information of children, etc.; and
  - Means of redress for personal rights.
- Means of effective monitoring and supervision:
  - Means of administrative monitoring and supervision, such as fines, recommendations, and orders;
  - Criminal penalties; and
  - Reporting of leaks, etc. and notification to the individual.
- How data utilization initiatives should be supported:
  - Data utilization that does not require individual consent; and
  - Promotion of voluntary initiatives in the private sector.

In June 2024, the commission published an "[interim report](#)". The interim report is a summary of the commission's views at that time, based on the discussions that had taken place up to that point.

This interim report was open to public comment, and [more than 2,000 comments were received](#). The commission continues to have further discussions based on the results of the public comments.

## IoT Product Security Conformity Assessment Scheme starting in March 2025

The Ministry of Economy, Trade and Industry (METI) released "[IoT Product Security Conformity Assessment Scheme Policy](#)" in August 2024.

In accordance with this policy, the [Information-Technology Promotion Agency](#) (IPA) will start operating the "Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR)" in March 2025.

IPA is [currently negotiating mutual recognition with relevant agencies](#) in Singapore (Cybersecurity Labelling Scheme), the United Kingdom (Product Security & Telecommunication Infrastructure Act), the United States of America (U.S. Cyber Trust Mark), and the European Union (Cyber Resilience Act).



## Outcome of an expert panel on the legal and regulatory framework for AI

In August 2024, [the Cabinet Office established the AI Institutional Research Group](#) as an expert panel under the AI Strategy Council to discuss the legal and regulatory framework for AI.

At the first meeting of the research group, [the Prime Minister outlined the following four basic principles](#):

- Balancing risk management and innovation promotion;
- Flexible system design to adapt to rapid changes in technology and business;
- International interoperability and compliance with international guidelines; and
- Proper procurement and utilization of AI by the government.

The interim report will be published based on the research group's discussion.

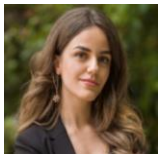
# Kosovo

## Contacts



**Ardian Rexha**

Legal Senior Manager, Deloitte Kosova  
[arrexha@deloittece.com](mailto:arrexha@deloittece.com)



**Vjollca Hiseni**

Legal Senior Associate, Deloitte Kosova  
[vhiseni@deloittece.com](mailto:vhiseni@deloittece.com)



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

## **Guidelines on collecting and usage of the biometric data in the private companies, including employee biometric data**

In line with the Law No.06/L-082 on Protection of Personal Data (Law on Data Protection), the Kosovo Agency for Information and Privacy (the Agency) has published some guidelines regarding the collection, processing and the use of biometric data with a noted focus on the biometric data on the private employment sector. The Law on Data Protection, stipulates that the private sector may only use biometric features if this is necessarily required for the performance of activities for the safety of people, the security of property or the protection of confidential data or business secrets. Employees must be informed in writing prior to the use of their biometric characteristics, about the intended measures and their rights.

The data controller shall however, prior to the introduction of measures using biometrics provide the Agency with a detailed description of the intended measures.

In light of this the employer is obliged to submit a request for authorization of the use of biometric data. The request shall include:

- Purpose of using biometric characteristics;
- Detailed description of the measures to be taken; and
- The information that will be provided to the data subject and the safeguards for protection of personal data.

Only after the employer accepts the authorization issued by the Agency, it can start with the use of biometric characteristics.

# Luxembourg

## Contacts



**Thomas Held**

Partner, Deloitte Legal Luxembourg  
theld@deloittelegal.lu



**Sophie Brisson**

Managing Director, Deloitte Legal Luxembourg  
sbrisson@deloittelegal.lu

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

## Recent amendments to GDPR implementation

- **Increased compliance:** National laws have been strengthened to better align with the GDPR regulation. This includes clarifications on the obligation to notify data breaches within 72 hours and increased responsibilities for data controllers and processors.
- **Enhanced role of DPOs:** Clarifications have been made regarding the qualifications and responsibilities of Data Protection Officers (DPOs), including their independence and involvement in all matters related to data protection.

## Legislation on data transfers

- **Schrems II:** Following the Schrems II ruling, Luxembourg has updated its laws to ensure that international data transfers to third countries are accompanied by appropriate safeguards. This includes standard contractual clauses, binding corporate rules and data protection impact assessments.
- **New requirements:** Specific directives have been issued for businesses concerning the use of cloud services and other international data transfers, ensuring practices comply with EU decisions and recommendations.

## Luxembourg Data Protection Authority (CNPD) guidance

- **Data subject rights:** Detailed guides have been published on how companies should handle requests from individuals regarding access, rectification, erasure and data portability.
- **Sensitive data:** Guidelines have been developed on handling sensitive personal data, including practical examples of what constitutes sensitive data and the conditions under which it can be processed.

- **Security measures:** The CNPD has issued recommendations on implementing appropriate technical and organizational measures to protect personal data, including the use of encryption, pseudonymization, and access management.

## Sector-specific guidelines

- **Finance:** Specific directives have been issued for the financial sector regarding the protection of client data, anti-money laundering measures, and transparency of information.
- **Healthcare:** For the healthcare sector, recommendations have been provided on managing electronic medical records, patient confidentiality, and security protocols.
- **Telecommunications:** Guidelines have been created to manage subscriber data, including data retention, protection against breaches, and user consent for marketing purposes.

## High-profile fines

- **Financial sanctions:** The CNPD has imposed significant fines, some amounting to millions of euros, on companies not complying with GDPR requirements, such as lacking a legal basis for data processing and violating data minimization principles.
- **Transparency:** Decisions and fines have been made public to encourage all companies to strengthen their compliance efforts and highlight the importance of adhering to data protection regulations.



## Notable enforcement actions

- **Audits and controls:** The CNPD has conducted regular audits and controls in companies to verify GDPR compliance. These audits include on-site inspections as well as reviews of internal policies and procedures.
- **Cease and desist orders:** In addition to fines, cease and desist orders have been issued requiring companies to modify their practices within strict deadlines, under the threat of additional sanctions.

## EU-US data privacy framework

- **New agreements:** Following the invalidation of the Privacy Shield, new agreements and mechanisms are being negotiated to allow secure data transfers between the EU and the United States, while ensuring an adequate level of protection.
- **Impact on businesses:** Luxembourgish businesses transferring data to the United States must closely follow these developments to ensure their data transfers remain compliant and involve appropriate safeguards as required by the CNPD and European authorities.



# ? What are the most relevant **cybersecurity updates**?

## Implementation of the NIS2 Directive:

### Adoption of new cybersecurity laws

- **Enhanced regulations:** Luxembourg has adopted new laws to align with the NIS2 Directive (Directive (EU) 2022/2555), which aims to strengthen cybersecurity across the EU. These new laws have broadened the scope of cybersecurity requirements to cover more sectors and introduce stricter security measures.
- **Sectoral expansion:** The updated laws now cover a wider range of sectors, including healthcare, energy, transport, and digital infrastructure, ensuring comprehensive protection against cyber threats.
- **Incident reporting obligations:** Organizations are now required to report significant cyber incidents within a 24-hour threshold, ensuring quicker response and mitigation.

### Strengthening cyber incident response

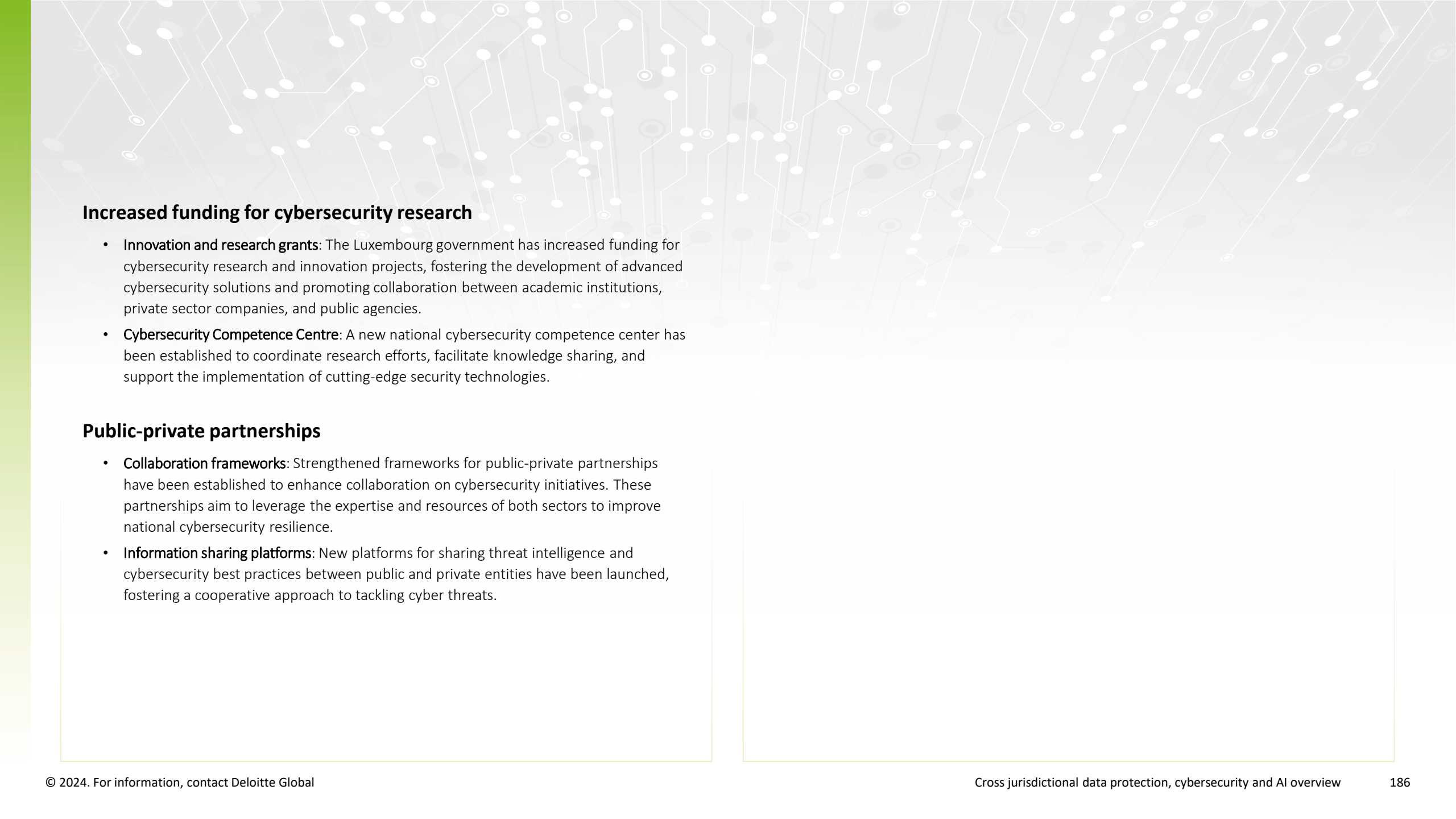
- **Incident management protocols:** The updated laws include detailed protocols for managing and responding to cybersecurity incidents. These protocols emphasize coordinated response efforts, rapid information sharing, and effective communication between affected parties and national authorities.
- **Increased penalties:** New compliance requirements come with increased penalties for non-compliance, creating stronger incentives for organizations to enhance their cybersecurity measures.

## Guidelines from the Cyber Security Agency Luxembourg (CIRCL)

- **Best practices for cyber hygiene:** CIRCL has published guidelines focusing on best practices for maintaining cyber hygiene, including measures for securing networks, managing passwords, and ensuring regular software updates.
- **Incident response guidelines:** Detailed guidelines for incident response have been issued, outlining steps to detect, analyze, and mitigate cyber threats effectively. These guidelines also emphasize the importance of maintaining robust incident response plans and conducting regular training exercises.

### Sector-specific cybersecurity guidelines

- **Healthcare sector:** Specific guidelines for the healthcare sector have been issued to address the unique challenges of protecting sensitive patient data and ensuring the integrity of medical systems against cyber threats.
- **Financial services:** In collaboration with the Commission de Surveillance du Secteur Financier (CSSF), guidelines have been developed for financial institutions to enhance their cybersecurity posture, focusing on risk management, threat detection, and incident response.
- **Energy sector:** The energy sector has received tailored guidelines emphasizing the protection of critical infrastructure, focusing on securing control systems and ensuring the resilience of energy supply chains against cyberattacks.



## Increased funding for cybersecurity research

- **Innovation and research grants:** The Luxembourg government has increased funding for cybersecurity research and innovation projects, fostering the development of advanced cybersecurity solutions and promoting collaboration between academic institutions, private sector companies, and public agencies.
- **Cybersecurity Competence Centre:** A new national cybersecurity competence center has been established to coordinate research efforts, facilitate knowledge sharing, and support the implementation of cutting-edge security technologies.

## Public-private partnerships

- **Collaboration frameworks:** Strengthened frameworks for public-private partnerships have been established to enhance collaboration on cybersecurity initiatives. These partnerships aim to leverage the expertise and resources of both sectors to improve national cybersecurity resilience.
- **Information sharing platforms:** New platforms for sharing threat intelligence and cybersecurity best practices between public and private entities have been launched, fostering a cooperative approach to tackling cyber threats.



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

## AI regulation preparation

- **Alignment with the EU AI Act:** Luxembourg has been preparing for the upcoming EU AI Act, which aims to regulate AI systems across the European Union. Discussions and preliminary national implementations have been undertaken to align Luxembourg with the proposed EU regulations. The Commission de Surveillance du Secteur Financier (CSSF), Luxembourg's financial sector regulator, has been particularly proactive, publishing research papers on AI that address its potential impacts and challenges. The CSSF continues to closely monitor AI deployment in the financial sector to ensure innovations are aligned with both consumer protection and industry competitiveness.
- **Public consultations:** The Luxembourg government has launched public consultations to gather opinions on how to implement these national regulations, ensuring that they address the concerns of citizens and businesses.

## Data protection and AI

- **Specific provisions:** Specific provisions have been introduced to ensure that AI applications comply with existing data protection laws, including the General Data Protection Regulation (GDPR).
- **Transparency and consent:** Companies must ensure transparency in AI-driven decision-making processes and obtain informed consent from users when their personal data is processed by AI algorithms.

## Government AI strategy

- **Promoting innovation:** The updated national AI strategy in Luxembourg emphasizes promoting innovation while ensuring that AI applications adhere to ethical and regulatory standards.
- **Supporting research:** The strategy includes measures to support AI research and development, creating a favorable environment for startups and tech companies.

## Ethical guidelines

- **Bias prevention:** The National Commission for Data Protection (CNPD) has published guidelines on the ethical use of AI, with specific recommendations to prevent biases in AI algorithms and has actively facilitated public engagement through consultations and interactive sessions, such as "DaProLab" workshops, promoting a well-informed dialogue on AI's regulatory landscape and ensuring stakeholder perspectives are considered in developing effective governance models.
- **Accountability and transparency:** The guidelines emphasize the importance of accountability and transparency in the development and use of AI systems. Companies must be able to explain how their algorithms make decisions and ensure they can be audited.

## Sector-specific AI guidelines

- **Finance:** For the financial sector, specific guidelines have been formulated to ensure that AI algorithms used meet security and data privacy standards for client data.
- **Healthcare:** In the healthcare sector, recommendations have been made for the use of AI in medical diagnostics, emphasizing patient data protection and transparency in AI-driven recommendations.
- **Smart cities:** For smart city projects, guidelines have been issued to ensure that AI systems used for urban management adhere to security and ethical standards.

## Compliance checks

- **Audits by CNPD:** The CNPD has conducted compliance checks on businesses and public institutions using AI technologies to ensure they adhere to data protection laws and ethical standards.
- **Focus on algorithms:** These audits focus on how AI algorithms are deployed, the use of data, and the security measures implemented.

## Sanctions for non-compliant AI use

- **Illegal data processing cases:** The CNPD has imposed sanctions on organizations that failed to comply with legal and ethical standards regarding AI usage, including cases of unlawful data processing or lack of transparency in AI-driven decisions.
- **Bias mitigation measures:** Sanctions also concern cases where adequate measures to prevent biases in AI systems were not implemented.

## Participation in EU AI initiatives

- **EU regulatory framework:** Luxembourg actively participates in EU-wide initiatives and discussions on AI, contributing to the development and shaping of regulatory frameworks like the AI Act.
- **Collaboration among member states:** Luxembourg collaborates with other EU member states to harmonize AI regulations and promote responsible AI development.

## Cross-border AI projects

- **Research and innovation:** Luxembourg is involved in cross-border AI research and innovation projects, leveraging its position within the EU to foster international collaboration. These projects often focus on advancing AI technologies while ensuring compliance with ethical and legal standards.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Data protection

### GDPR compliance

Continued emphasis on strict compliance with the General Data Protection Regulation (GDPR) as well as ongoing adjustments and improvements in data protection practices and policies.

### Data Protection Officers

Increasing importance and role of Data Protection Officers (DPOs) in organizations to ensure adherence to data protection laws and to oversee data processing activities.

### Enhanced regulatory enforcement

More stringent enforcement actions and increased fines by the National Data Protection Commission (CNPD) for non-compliance with data protection regulations.

## Cybersecurity

### National cybersecurity strategy

Implementation of Luxembourg's national cybersecurity strategy, emphasizing the protection of critical infrastructure, enhancing cyber resilience, and promoting a secure digital economy (Bill No. 8364/02 concerning measures to ensure a high level of cybersecurity and amending several laws).

### Certification and standards

Adoption of EU-wide cybersecurity standards and certifications (Cybersecurity Act), promoting higher security standards across sectors.

## Public-private partnerships

Strengthening collaborations between government agencies and private companies to address and combat cyber threats more effectively.

## Sophisticated threat detection

Enhanced use of advanced threat detection technologies, such as AI and machine learning, for early identification and mitigation of cyberthreats.

## AI

### AI regulation and ethics

Development of national guidelines and frameworks in alignment with European-wide regulations to ensure ethical AI usage, transparency, and accountability in AI systems.

### Investment in AI research

Increased funding and support for AI research and development initiatives, fostering innovation and encouraging startups and tech companies to explore AI applications.

### AI in public services

Integration of AI technologies into public services to improve efficiency, service delivery, and decision-making processes.

### Data-driven policies

Utilization of AI and data analytics in policymaking to derive insights and formulate more effective and evidence-based policies.

# Mexico

## Contacts



**Mauricio Oropeza**

Partner, Deloitte México  
[moropeza@deloittemx.com](mailto:moropeza@deloittemx.com)



**Melissa Franco**

Manager, Deloitte México  
[melfranco@deloittemx.com](mailto:melfranco@deloittemx.com)

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

## **Supreme Court criteria on the accountability on asset management in union matters**

In 2021, several unions filed an amparo trial against the obligation of the union leadership to render a complete and detailed account of the administration of their assets to their members, as they considered that it implied a violation of the right to safeguard the personal data of the union association.

As a result of the analysis of the Supreme Court of Justice of the Nation, through jurisprudential thesis [2a./J. 10/2021 \(10a.\)](#) it is resolved that this obligation does not violate the right of access to information and protection of personal data since the directive of the unions is obliged to observe the provisions of the Federal Law on the Protection of Personal Data in Possession of Private Parties regarding the processing of the union's data, considering that, by virtue of the principle of representativeness of its members is their obligation to provide to its members the information on the assets of the union and its administration, as they are the ones who integrate it and cover the contribution or membership fees.

## **Permissibility of taking photographs of school directors and staff in the event of a visit by the verifying authority**

The General Education Law authorizes the educational authority to, in the case of making a visit of the private education facilities and, prior to notification of the individual in question, take photographs or video of the staff, teachers and directors to support the visits they make, implementing the relevant measures for the use and protection of personal data.

In this sense, the Supreme Court established in the jurisprudential criterion [2a./J. 22/2021 \(11a.\)](#) that said provision does not violate the right to protection of personal data, as it is justified upon verifying the requirements for the operation and conditions of safety and efficiency of said schools, without exempting the authority from observing the provisions of the applicable data protection regulation.

## **INAI to issue regulations on administrative sanctioning law**

The Supreme Court determined that the constitutional jurisdiction granted to the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) to hear the matter of protection of personal data in the possession of individuals grants it powers, among which is the prerogative to issue general rules, both substantive and adjective, regarding the protection of personal data, to the extent that, as an autonomous constitutional body, it must have the necessary tools to the fulfillment of their constitutional duties.

From this perspective, [the INAI has powers to issue regulations that detail its verification processes and imposition of sanctions](#), provided that they have a direct and immediate relation with due observance of the right of access to public information and the protection of personal data in possession of the obligated subjects.

## **Notices to the tax authorities regarding partners or shareholders and similar positions of legal entities**

The Federal Tax Code establishes [the obligation of the legal entities to file, as applicable, the notices with the information of its shareholders](#), members or partners, at the time of incorporation or any entry or exit of them.



However, the Supreme Court ruled that such obligation does not violate the data protection right, as they are required in order to verify and avoid the incorporation of “billing entities” used for the simulation of transaction and fiscal evasion/fraud, which implies that the tax authorities need some minimum information of its shareholders, partners or members or similar in order to be able to apply any sanctions or penalties that might arise. However, by the principle of necessity, such information is deemed suitable and subject to the rules and exceptions provided for in the regulations applicable to transparency and protection of personal data.

### **Obligation to provide the geolocation of the employer's address in the case of specialized service providers**

As a result of the prohibition of outsourcing in Mexican labor legislation, the Public Registry of Contractors of Specialized Services or Specialized Works was established, in which, as part of the registration requirements, [it is requested that geolocation be provided on the computer platform at the time of registration](#).

In this sense, the Supreme Court resolved that this requirement is incorporated in order to avoid the registration of non-existent or simulated companies, without such geolocation being able to be carried out in real time, so there is no violation of the protection of personal data, since, although the registry is available for public consultation on the internet portal of the Ministry of Labor and Social Welfare, in the collection and processing of all the information in the register, the regulations on transparency, access to information and protection of personal data must be observed.

### **Legal requirements for disclosure of telecommunications data**

The Supreme Court has resolved [requests made by the Public Ministry to telecommunications licensees regarding the identity and address of subjects under investigation](#) as well as the type of communication (voice transmission, voicemail, conference or data, supplementary services, communication services, messaging or multimedia used), and the data necessary to determine the date, time and duration of the communication, are included within the scope of protection of the right to the inviolability of private communications, therefore, in order for the concessionaire to proceed with its disclosure to the ministry, it is essential that there be a resolution from the competent federal judicial authority.

### **Access to personal data concerning deceased holders**

The INAI, the guarantor body in matters of personal data protection, established through agreement [ACT-PUB/25/09/2024.06](#) that it is possible to authorize access to personal data contained in a clinical file of deceased persons provided that a legal or legitimate interest is accredited. To this end, the INAI would proceed with the analysis of each specific case once the admissibility of said clinical file has been denied by the person responsible for its treatment.

### **Cellphones and mobiles of public officers**

The INAI solved through agreement that [the cellphone numbers of public officers will be deemed as public information](#) in case it is provided as a labor benefit of such officer, as public resources are used and being such mobile, property of the government agency or body that provides it to the public officer.



# ? What are the most relevant **cybersecurity updates?**

## Project of a Federal Cybersecurity Law

To date, there is no law in cybersecurity matters in Mexico. However, in 2023, a project for the issuance of a Federal Cybersecurity Law was submitted for analysis. Even if such law has not been approved, the project, in general terms, considers:

- The powers, attributions and coordination of public and private sector in cybersecurity matters and the foundations of the prevention and prosecution of cybersecurity crimes.
- The rights and obligations of the users of the cyberspace, establishing, among others: (i) the right to electronic commerce, protection of the digital identity and privacy, and (ii) the obligation to use the digital services only for lawful purposes and cooperate with the authorities in the investigation in cybersecurity matters as well as pentesting.
- The incorporation of a National Cybersecurity Agency, an Intersecretarial Commission on Information and Communication Technologies, and Information Security, a National Center for the Response of Cybernetic Incidents, and a National Registry of Cybersecurity Incidents.
- The obligation of providers of digital infrastructure services (social media, streaming platforms, online gaming communities, online entertainment platforms and telecommunications) to have at least one legal representative based in Mexico, register before the National Cybersecurity Agency, open a cybersecurity compliance unit and have the applicable policies, procedures and measures for the response to cybersecurity incidents.
- For providers of financial and banking services, the obligation to have the cybersecurity measures to avoid electronic frauds.
- The registration in the National Registry of Technology Providers for Communications Intervention of developers of equipment, medium, device, or software resulting from technological evolution that allows the exchange of data, information, audio, video, messages, as well as electronic files that record, preserve the content of conversations or register data that identifies the communication, which can be presented in real time.



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

## **Project of Law on Ethical Regulation of Artificial Intelligence and Robotics**

As for AI matters, there is no specific law for AI in Mexico yet, however, a project of law was filed in 2023, containing, in general terms:

- Establishes the guidelines of public policies in the Mexico for the ethical regulation of the use of artificial intelligence and robotics within the national territory;
- Regulates and standardize the use of AI and robotics in their use for purposes governmental, economic, commercial, administrative, communicational and financial so that its use is always based on adherence to ethics and adherence to law; and
- Creates and regulates the Mexican Council of Ethics for Artificial Intelligence and robotics (*Consejo Mexicano de Ética para la Inteligencia Artificial y la robótica*, or Cmetiar) and the National Statistics Network for the use and Monitoring of Artificial Intelligence and Robotics (*Red Nacional de Estadística de uso y monitoreo de la Inteligencia Artificial y la Robótica*).



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## AI and cybersecurity regulation

### Project of Law on Ethical Regulation of Artificial Intelligence and Robotics

It is expected that the review process of this project is resumed in 2024 for its discussion and approval in 2025.

### Draft Federal Cybersecurity Law

It is expected that the review process of this project is resumed in this period of legislative bodies.

## Amend to the data protection and telecom guarantor bodies

On 23 August 2024, the project containing the proposal for constitutional amend regarding organic simplification was approved by the Constitutional Points Commission of the Chamber of Deputies.

This amend would imply that, if approved in its entirety, the INAI and the Federal Telecommunications Institute (IFT) would be eliminated, reassigning their functions to other government bodies of the centralized public administration, which might result in a comprehensive restructuring of the regulations on the subject and the existing criteria.



# Morocco

## Contacts



**Grégoire Chaste**

Partner, Deloitte Conseil  
[gchaste@deloitte.com](mailto:gchaste@deloitte.com)



**Amal Barhon**

Legal Manager, Deloitte Conseil  
[abarhon@deloitte.com](mailto:abarhon@deloitte.com)



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

Moroccan data protection law has not changed since 2009. It remains governed by Law No. 09-08 (promulgated by Dahir No. 1-09-15), which provides a legal framework for the protection of personal data. This law regulates data collection, processing, and sharing, ensuring that personal data is handled lawfully, transparently, and securely.

## **Greater focus on cross-border data transfers**

Morocco's regulatory environment is expected to focus more on international data transfers as global data flows increase.

Under Article 44 of Law 09-08, data transfers are allowed only when the destination country provides an adequate level of protection. Future developments may include clearer guidelines on data transfer mechanisms, such as binding corporate rules (BCR) or standard contractual clauses (SCC), aligning Morocco with international practices.

## **Key rules for data collection and processing**

- **Prior declaration:** Mandatory for non-sensitive data processing;
- **Prior authorization:** Required for sensitive data or specific cases like genetic data or criminal records; and
- **Appointment of data controllers:** Data controllers must be appointed to ensure compliance with the law.

## **First Atlantic Inter-Network Meeting of Data Protection Authorities**

**The first Atlantic Inter-Network Meeting of Data Protection Authorities was a significant event organized by Morocco's National Commission for the Control of Data Protection (the CNDP)**

This high-level meeting took place in Rabat and focused on strengthening collaboration and addressing challenges in the field of data protection.

Key topics discussed were:

- **Neurodata and neurotechnology:** Addressing the ethical concerns and regulatory frameworks for protecting personal data derived from neural technologies;
- **Digital identity for public services:** Exploring secure and efficient methods for using digital identity to access public services; and
- **Artificial intelligence (AI) and deep fakes:** Discussions on safeguarding personal data in AI advancements and mitigating risks associated with deep fakes.



## **Launch of the National Data Protection Register**

**In June 2023, Morocco's National Commission for the Control and Protection of Personal Data (CNDP) launched the National Register for the Protection of Personal Data.**

This public register provides transparency about the management of personal data and allows data controllers to submit updates or corrections to their entries. The register also aims to foster a climate of digital trust in the country. This is a significant step in enhancing compliance with data protection regulations and improving public access to data governance information.

## **Investigation of data breaches**

### **Data breach of TLS contact**

In January 2023, the CNDP launched an investigation into TLS contact, a company handling visa applications for foreign embassies, after it reported a data breach. This incident highlighted the growing concerns around data protection in Morocco, particularly for companies handling sensitive personal data. The CNDP's proactive approach to data breaches shows its commitment to enforcing data protection laws and ensuring that organizations are held accountable.

## **Global appeal to tech giants on data scraping**

In August 2023, the CNDP joined an international initiative with 11 other data protection authorities, addressing major tech companies like Google, Meta, and TikTok. The joint statement warned against the risks of data scraping, a practice where automated systems extract user data without consent. This call to action emphasized the importance of safeguarding personal data on global platforms and urged companies to implement stronger data protection measures.

# ? What are the most relevant **cybersecurity updates**?

Moroccan cybersecurity law has not changed since 2020. It remains governed by Law No. 05-20 (the Cybersecurity Law) (promulgated by Dahir No. 1-20-69), which provides a legal framework for the protection of information systems and cybersecurity. This law regulates the security of information systems and cyber incident management, ensuring that sensitive information is handled securely, with robust protection measures for critical infrastructure and compliance with national guidelines.

## **Key rules for cybersecurity management and incident handling**

### **Appointment of security officers**

Credit institutions and critical infrastructures are required to appoint a security officer responsible for managing and overseeing the cybersecurity policy and compliance with the law. This officer serves as the contact person for the General Directorate of Information Systems Security (DGSSI) and ensures the entity's readiness for audits and incident reporting.

### **Mandatory audits and security approvals**

Entities must undergo mandatory cybersecurity audits to ensure their systems comply with national guidelines. Sensitive systems require security approval from the DGSSI before they can be deployed. Audits are conducted by qualified service providers approved by the DGSSI, and the audit results must be followed by corrective actions.

## **Classification of information assets**

Under Articles 5 and 17 of the Cybersecurity Law, all information assets must be classified based on their sensitivity concerning confidentiality, integrity, and availability. The classification helps determine the protection measures that need to be applied, ensuring that the most critical systems receive the highest level of security.

## **Incident reporting and handling**

Entities are required to implement systems for monitoring and detecting cybersecurity incidents. In the event of an incident, they must immediately notify the DGSSI and provide any necessary technical information to address the threat.

## **Outsourcing restrictions and national data hosting**

The law strictly requires that sensitive data be hosted exclusively within Morocco. If an entity needs to outsource its information systems, it must do so through DGSSI-approved service providers.



## **Update of the National Information Systems Security Directive (DNSSI-V.2)**

On 12 January 2023, the General Directorate of Information Systems Security (DGSSI) updated the National Information Systems Security Directive of 2014, through Circular No. 02/2023. This update aims to incorporate recent changes in the legal and regulatory framework while taking into account international best practices in the field of information systems security.

## **Rising cyber threats and national defense efforts**

In 2023, Morocco faced significant cyberthreats, with over 52 million cyberattacks blocked, according to Trend Micro's annual report. These attacks included more than 40 million email threats and 1.6 million malicious URL attacks. The country remains a prime target for cybercriminals, and sophisticated techniques are increasingly being used for financial gain. The rise in cyber incidents led to a growing emphasis on national cybersecurity strategies and investments in digital defenses.

## **Memorandum of Understanding with the UAE**

Morocco has significantly improved its position in the Global Cybersecurity Index published by the International Telecommunication Union (ITU). Achieving a score of 97.5/100, the country now ranks in the top tier (Tier 1), reflecting substantial progress in legal frameworks, technical measures, capacity-building, and international cooperation in cybersecurity. This achievement demonstrates Morocco's ongoing commitment to strengthening its national cybersecurity strategy and resilience.

## **Increased focus on combating cybercrime**

In June 2024, Morocco reiterated its commitment to tackling cybercrimes. The CNDP has taken several steps to modernize and protect digital infrastructures from cyber threats, focusing on raising public awareness and introducing tighter regulations against cybercriminal activities.





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

## **Absence of AI legal framework in Morocco**

Currently, Morocco has no specific legal framework governing artificial intelligence (AI). The country is yet to develop laws or regulations addressing AI governance, ethics, or liability, although AI is increasingly recognized as a critical area requiring future regulation. The lack of a formal structure highlights the need for a robust regulatory framework to address challenges such as data privacy, algorithmic transparency, and accountability.



# What are the most relevant expected developments in data protection, AI and cybersecurity?

## Strategic pillars for developing the cybersecurity framework in Morocco by 2030

### National Cybersecurity Governance: institutional and legal framework

The primary goal is to strengthen the legal and regulatory framework for cybersecurity while improving national coordination mechanisms. This includes drafting laws that address the challenges of cyberspace and aligning institutional efforts to ensure a coherent and effective response to cyberthreats.

### Security and resilience of the national cyberspace

This initiative aims to support decision-making through data-driven policies and promote the implementation of internationally recognized cybersecurity standards and norms. It also focuses on enhancing national capacities for the prevention, management, and response to cyber incidents and crises, as well as protecting the information systems of critical infrastructures.

### Capacity building and awareness

Developing a cybersecurity culture within Moroccan society is crucial. This involves awareness campaigns targeting citizens, the public, and private sectors, along with introducing cybersecurity modules in school curricula. Additionally, the initiative seeks to support the national cybersecurity ecosystem by promoting research and innovation within universities and training centers, while enhancing the skills of cybersecurity professionals.

### Regional and international cooperation

It is essential to strengthen Morocco's active participation in regional and international forums on cybersecurity. This also includes developing bilateral cooperation with other countries in areas such as information sharing and capacity building in cybersecurity.

## Morocco on the verge of a technological revolution: artificial intelligence at the core of national development

Morocco is increasingly positioning itself as a key player in the field of AI in Africa. By 2023, Morocco has risen to fourth place in Africa and 88th place worldwide in terms of AI readiness, according to the government's Artificial Intelligence Readiness Index addressed by Oxford. Innovative initiatives driven by universities and research centers, coupled with the rise of AI in both public and private sectors, demonstrate the kingdom's commitment to integrating this technology into its development strategies.

### Toward ethical AI governance: Morocco's central role on the international stage

The adoption of ethical governance for artificial intelligence is a priority for Morocco. The kingdom seeks to balance technological innovation with respect for human values, adhering to a rigorous legal framework while playing an active role in international discussions on the future of AI.

### AI diplomacy: Morocco tackling global challenges

Morocco aims to integrate AI into its diplomacy, aligning it with global challenges such as climate change and international security. This approach would enhance the kingdom's visibility and influence on the international stage, particularly within multilateral institutions.

# Nigeria

## Contacts



**Asiata Agboluaje**

Partner, Deloitte Nigeria

[aagboluaje@deloitte.com.ng](mailto:aagboluaje@deloitte.com.ng)



**Inepaimi Ayah**

Manager, Deloitte Nigeria

[iayah@deloitte.com.ng](mailto:iayah@deloitte.com.ng)

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

## **Nigeria Data Protection Act 2023**

One significant data protection update is the enactment of the Nigeria Data Protection Act 2023 (NDPA) which was signed into law on 12 June 2023 as the principal law governing data protection in Nigeria.

The NDPA also established the Nigeria Data Protection Commission (NDPC) as the regulatory authority administering the NDPA and overseeing data protection and privacy issues in Nigeria.

## **Nigeria Data Protection Commission Guidance Notice on the Filing of Data Protection Compliance Audit Returns 2023**

The NDPC Guidance Notice on Filing of Data Protection Compliance Audit Returns (CAR) was released by the NPDC in 2023 to clarify the requirement for filing of compliance audit returns, which is an obligation for data controllers and data processors under the Nigeria Data Protection Regulation (NDPR) 2019.

The guidance notice also highlights the role of Data Protection Compliance Organizations (DPCOs) in facilitating the filing of CAR with the NPDC, the CAR focus areas and effect of non-compliance.

## **Nigeria Data Protection Commission Code of Conduct for data protection compliance organizations (DPCOs) 2023**

NDPC released the Code of Conduct on 15 December 2023 to, amongst others, foster discipline and uphold accountability among DCPOs. Amongst others, the code of conduct provides for the compliance services that may be rendered by a DPCO, the DPCO's responsibility to data subjects, the DPCO's responsibility to the NDPC, the DPCOs responsibility to clients (data processors and data controllers), as well as the DPCOs responsibility to other DPCOs. The code of conduct also outlines the grounds for the revocation of the license of a DPCO.

## **Nigeria Data Protection Commission Guidance Notice on the Registration of Data Controllers and Data Processors of Major Importance 2024**

On 14 February 2024, the NDPC, pursuant to the NDPA, released a Guidance Notice on the Requirement of Registration for Data Controllers and Data Processors of Major Importance (Guidance Notice). Highlights of the notice include designation of data controllers and processors of major importance, and classification of data controllers and data processors of major importance. Deadline for registration was fixed as 30 June 2024 but was extended to 31 October 2024. Registration after the due date will be treated as a default which is liable to penalty.





## **Central Bank of Nigeria (Customer Due Diligence) Regulations 2023**

The Central Bank of Nigeria Customer Due Diligence Regulations 2023 was issued by the Central Bank of Nigeria on 31 May 2023 pursuant to the provisions of Nigeria’s anti-money laundering legislations. The regulations contains provisions requiring banks to request for, amongst others, personal data of prospective customers as part of its customer identification process.

## **Incorporated Trustees of Ikigai Innovation Initiative vs. National Information Technology and Development Agency (Suit No. FHC/ABJ/CS/1246/2022)**

The Federal High Court (FHC) delivered a judgement on 28 November 2023 which addressed two primary issues: the adequacy of the “allow list” issued by the then data protection regulator, National Information Technology Development Agency (NITDA), pursuant to the NITDA Implementation Framework and the validity of the standard contractual clauses (SCCs) and binding corporate rules (BCRs) as cross-border transfer mechanisms. Some aspects of the decision is however now rendered moot with the enactment of the NDPA.

# ? What are the most relevant **cybersecurity updates?**

## **Cybercrimes (Prohibition, Prevention, ETC) (Amendment) Act 2024**

This act was signed into law on 28 February 2024 to amend the Cybercrime (Prohibition, Prevention, ETC) Act 2015 (Cybercrime Act). In addition to other matters, the amendment inserted some consequential words that were inadvertently omitted in the Cybercrime Act.

The act also amends the Cybercrime Act to allow the use of electronic signature for certain categories of contractual transactions or declarations and documents, provided certain conditions are adhered to.

Further, the act provides for verification of the identity of customers of financial institutions carrying out electronic financial transactions.



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

## **National Artificial Intelligence Strategy 2024**

The National Artificial Intelligence Strategy (NAIS) was released by the Federal Ministry of Communication, Information and Strategy in August 2024 as part of Nigeria’s strategy “to be a global leader in harnessing the transformative power of AI through responsible, ethical, and inclusive innovation....”. NAIS contains provisions aimed at ensuring a sound artificial intelligence (AI) spectrum. It further provides an implementation strategy and risk mitigation strategies.



# What are the most relevant expected developments in data protection, AI and cybersecurity?

## Proposed data protection reforms

There is the expectation that the NDPA General Application and Implementation Directive (NDPA GAID) Drafting Committee will release its directive in the coming months. Already, a draft NDPA GAID has been issued by the NDPC earlier in October 2024 and expectations are that same will be finalized and the final version released in a few months' time.

Also, following the court's decision in *Ikigai's* case, there is the expectation that the NDPC will revise the approved list of countries with adequate data protection laws and incorporate a country-by-country assessment as mandated by the court.

Further, there is currently before the Nigerian National Assembly a bill to repeal and re-enact the National Identity Management Commission Act No. 23 of 2007. The bill seeks to, amongst others, reinforce the regulatory functions of the National Identity Management Commission as well as expand the scope of registrable persons under the National Identity Management System.

## Proposed artificial intelligence reforms

There is currently a bill on "Control of Usage of Artificial Intelligence Technology in Nigeria Bill" before the National Assembly aimed at codifying the legal and institutional framework for the regulation of artificial intelligence in Nigeria. The bill has already undergone first reading at the Federal House of Representatives and it is hoped that the bill will be passed in the near future. Other bills currently before the National Assembly include:

- The National Institute for Artificial Intelligence and Robotic Studies, Somolu, Lagos State (Est) Bill 2023; and
- The Federal Artificial Intelligence Institute (Establishment) Bill 2023

## Proposed cybersecurity reforms

There is also the "Closed Circuit Television Bill" before the Nigerian National Assembly seeking to compel the compulsory installation of closed-circuit television in private buildings and offices. The aim is to achieve an integration of private closed circuit television infrastructure into the Nigerian national security network.



# Norway

## Contacts



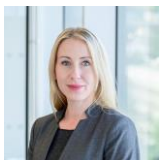
**Bjørn Ofstad**

Partner, Deloitte Advokatfirma  
[bofstad@deloitte.no](mailto:bofstad@deloitte.no)



**Hanne Pernille Gulbrandsen**

Partner, Deloitte Advokatfirma  
[hgulbrandsen@deloitte.no](mailto:hgulbrandsen@deloitte.no)



**Eirin Helen Hauvik**

Partner, Deloitte Advokatfirma  
[ehauvik@deloitte.no](mailto:ehauvik@deloitte.no)

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

## **New National Digitization Strategy**

### **Privacy is a central focus, specifically regarding built-in privacy**

The Norwegian government will ensure privacy in all digitalization efforts by 2030. All relevant IT solutions in the public sector must have built-in privacy, and the government will ensure citizens' privacy when dealing with major tech giants.

## **Fine issued to university in Agder**

### **On 4 September 2024, the Norwegian Data Protection Authority issued a fine of NOK 150,000 to a university in Agder for data protection breaches**

Documents containing personal data was stored on public Microsoft Teams channels, meaning they were open to anyone with an email address from the organization. Employees without a professional need have therefore had access. The university had not implemented appropriate measures to ensure the security of personal data in its use of Microsoft Teams. The breach had been ongoing since the university began using Microsoft Teams in August 2018.

The breach involves documents containing personal data of employees, students and external parties. Around 16,000 individuals have been affected. The affected data includes, among other things, names, personal identification numbers, information about accommodations for exams, the number of exam attempts, and special arrangements.

Additionally, the non-compliance involved a list of refugees from Ukraine associated with the university, containing information such as contact details, education, and residency status.

The university has not appealed the fine.

## **Fine issued to the Norwegian Labour and Welfare Administration**

### **On 18 March 2024, the Norwegian Data Protection Authority (Datatilsynet) issued a fine of NOK 20 million to the Norwegian Labour and Welfare Administration (NAV) following an audit of their data confidentiality practice.**

The investigation revealed deviations in NAV's control over access to personal data and its logging procedures. The fine is one of the largest imposed on a public entity in Norway.

The Data Protection Authority highlighted that NAV's handling of personal data exhibited structural and organizational weaknesses. They concluded that NAV lacked sufficient oversight and understanding of the necessary privacy protections. As a result, the authority also mandated several corrective actions for NAV to improve its data protection practices.

NAV has appealed the fine to the Privacy Appeal Board.

## **Collaborative Nordic Principles on children's privacy in online games**

**The goal of the principles is to strengthen children's specific rights to protection under GDPR when they are engaging in online gaming platforms**

The principles were developed collaboratively by the Nordic data protection authorities after a decision was made in 2022 to establish a working group to address issues related to children and online gaming.

The guidance aims to make game developers aware of some of the assessments they must undertake under privacy regulations when processing children's personal data. Four key privacy principles have been selected as a starting point for the assessments the data controller must conduct:

- The principle of fairness;
- The principle of transparency;
- The principle of data minimization; and
- The principle of accountability.

## **Ruling by Oslo District Court – 23-160384-TOSL/04**

**1 July 2024, Oslo District Court upholds Norwegian DPA fine against the social network app, Grindr**

On 13 December 2021, the Norwegian Data Protection Authority (DPA) fined Grindr a fine of €6.4 million for disclosing personal data to advertising partners without a valid legal basis (Article 6(1) GDPR) and for disclosing special categories of personal data. The sharing of data included GPS location, IP address, advertising ID, age, gender and sexual orientation by having a profile in the app. Users could be identified through the shared data, and the recipients could potentially share the data further.

The court agreed with the DPA that the app disclosed sexual orientation and relationship under GDPR Article 9(1). Further on, the court upheld that consent was not freely given under GDPR Article 4(11), as there was no real freedom by choice. The court stated that Grindr failed to use clear language, making it difficult for users to understand what they were consenting to and what the consequences was. The court found that Grindr consciously chose to be in breach with GDPR, because other alternatives to obtaining consent was too expensive or complicated. Even if Grindr did not have any choice but to obtain consent in the way they did, they still did not fulfil the requirements for information to the data subject for it to be a valid consent.

Due to the seriousness of the breach and the large amount of data subjects that was affected, the court did not find a basis for reducing the fine from the DPA.

Grindr has appealed the ruling.



# ? What are the most relevant **cybersecurity updates?**

## **Proposal for regulations to the new Digital Security Act**

**The Digital Security Act, together with the proposal for regulations on digital security, will implement the NIS1 Directive. Where appropriate, the ministry has attempted to align with the requirements of the NIS2 directive**

On 11 September 2024, the Ministry of Justice and Public Security sent a proposal for regulations to the Digital Security Act for consultation. The consultation deadline is 11 December 2024. In summary, the requirements for providers of critical societal services include:

- A security management system based on recognized standards;
- Prepared risk assessments;
- A plan for risk management;
- Organizational security measures (instructions and procedures);
- Technological security measures adapted to the scope, complexity, operational environment, user environment, function, and risk;
- Physical security measures;
- Security measures for personnel; and
- Contingency plans and incident management.

The obligation to notify constitutes: 24 hours after becoming aware of the incident, an update after 72 hours, and an incident report within one month from the notification.

Supervision can be carried out if there is a risk of violations and the supervisory authority deems it necessary. The Norwegian National Security Authority (NSM) will likely be the supervisory authority. Administrative fines can amount to up to 4% of the total annual turnover in the preceding financial year.

It is proposed that the regulations enter into force immediately.

## **Ruling HR-2024-990-A by the Norwegian Supreme Court**

**Current regulation of security systems for payment services do not include requirements to have systems or routines in place to discover or counteract fraud against customers when the customers themselves authorize the payment.**

A CEO of a Norwegian subsidiary of Edison International S.p.A. transferred approx. NOK 130 million (or €11.3 million) to two bank accounts in Hong Kong, as part of what they thought was a top-secret business deal ordered by the CEO of the mother company. The imposters used social manipulation – an email address closely resembling the CEO's address with instructions to only reply in writing – to get the CEO to instruct the bank to transfer the money. The imposters were caught but the money was gone and the question put before the Supreme Court was whether the bank (Danske Bank) was liable for Edison's loss.

One question the Supreme Court answered was whether the regulation of systems for payment services (FOR-2019-02-15-152), which implements Article 95 of EU Directive 2015/2366, entails a duty for banks to have IT systems in place for the detection this type of fraud. The Supreme Court's answer was negative: the regulation does not entail a duty to have IT systems or control routines in place to detect fraud when the customer authorizes the payment per email.



## Revisions of the Financial Institutions Act

### New § 2-1 – The right to pay with cash

Among other things, the right to pay with cash was justified by security concerns related to digital attacks on payment systems. Adequate cash circulation was considered as a backup system in the event of digital attacks. Consequently, businesses are now forced to accept cash.

The new regulation was enforced 1 October 2024 and specifies that businesses operating out of a venue where they sell goods or services regularly, must generally provide consumers with the choice to pay with cash.

Part of the reason behind this change was to create a more resilient payment infrastructure in the event of a cyberattack or similar catastrophe knocking out the digital payment infrastructure.

Prop. 55 L (2023-2024) p. 30 (our translation): "The ministry refers here to the consultation statement from the Central Bank of Norway, which points out that cash is ultimately the only alternative if the digital payment systems are down or unavailable. As an example of such situations arising, prolonged power outages, system failures, and digital attacks on payment systems and banks can be mentioned."

## E-Com regulations

### § 7-6 - Enforced 1 September 2023

The legal provision outlines the obligations of service providers under the Electronic Communications Act (E-com Act). It requires providers to promptly store information specified in the law, ensuring adequate security to prevent data loss.

Upon request from the police or prosecution authority, providers must promptly disclose the stored information, with response time depending on the request's scope and complexity.

Providers must also ensure secure data disclosure and use standardized data exchange solutions where possible.

Additionally, providers must establish a contact point for police communication and report IP address allocations to The Norwegian Communications Authority (Nkom). Annually, providers must prepare a cost overview of the disclosure obligation, confirmed by an auditor, to be submitted to Nkom upon request.

Overall, § 7-6 mainly requires providers of electronic communications to “ensure” that data is not lost.



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

## **Guidance on AI in the public sector**

**The Norwegian Digitalisation Directorate has published guidance for responsible use and development of AI**

The background is that many documents and resources can provide guidance on AI, but it can be difficult to navigate. The guidance is intended to provide concrete advice to those who are to develop and use AI in the public sector. The guidance is not exhaustive but intends to help the public sector to quickly identify and address challenges related to AI.

## **Plan for safe and efficient use of AI in the health sector**

**The Norwegian Health Directorate is leading the work to facilitate the safe introduction of AI in the health sector**

On 13 August 2024, the Norwegian Health Directorate published a report with a common AI plan for what measures should be implemented in 2024-2025 to support the needs of health trusts and municipalities. Together, the activities in the common AI plan for health and care services will contribute to achieving the goal of increasing the use of AI solutions that are safe and sustainable, contribute to health and care services of equal or better quality, streamline resource use and free up time for health personnel.

## **AI report**

**The Confederation of Norwegian Enterprise (NHO) has published a report on AI in Norway**

The report discusses the benefits of AI, with particular emphasis on the value creation that can be achieved if businesses in the public and private sectors utilise the opportunities. The report also discusses challenges and barriers that society must be aware of going forward, so that businesses can utilize AI in a safe and responsible manner.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Implementation of Digital Operational Resilience Act (DORA)

DORA is an EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025. DORA sets uniform requirements for the security of network and information systems of companies and organizations operating in the financial sector as well as critical third parties which provide information communication technology (ICT)-related services to them.

EU regulations are implemented in Norway through the EEA agreement. Since DORA is a regulation, Norway cannot adjust the regulations beyond what is stipulated in the national choices in the regulation and the EEA agreement.

On 23 January 2024, the Norwegian Ministry of Finance issued a consultation document on the need for changes in Norwegian law to implement the expected EEA obligations corresponding to DORA. It was proposed that the regulation should be implemented through a law on digital resilience in the financial sector. The deadline for the consultation was 3 April 2024.

Norway can choose to implement DORA before its inclusion in the EEA agreement. Simultaneous implementation with the EU could be appropriate for businesses with cross-border operations. The implementation date in Norway is not yet confirmed.

## Proposal for regulations to the Digital Security Act open for consultation

It is proposed that the regulations enter into force together with the Digital Security Act “immediately”. The Digital Security Act, together with the proposal for regulations on digital security, will implement the NIS1 Directive. Certain aspects of the act and proposal will align with the requirements of the NIS2 Directive. The consultation deadline is 11 December 2024.

## Follow-up review of the Personal Data Act (Personopplysningsloven)

**The Ministry of Justice and Public Security is requesting input for the follow-up review of the Personal Data Act, with a deadline for responses on 1 November 2024**

The purpose of the follow-up review is to assess whether the rules in the Personal Data Act, including the transitional rules and regulations, have an appropriate design and function satisfactorily, especially in light of developments since the law's adoption in 2018, or whether there is a need for changes or new rules.

## Act relating to electronic communications

**Proposal for the new E-com Act was presented on 12 April 2024**

This act regulates the provision and use of networks and services that allow us to communicate electronically through mobile phones and the internet. The proposed legislation aims to enhance information security by extending the requirement for adequate security from electronic communications providers to also include data center operators. Furthermore, it tightens the consent requirements for cookies, strengthens consumer rights, regulates the data center industry, and introduces a provision that enables authorities to mandate broadband delivery in areas where it is not otherwise available.

The latest update from the Norwegian parliament is that the act will not be considered until the autumn, so it will not come into effect until 1 January 2025 at the earliest.

# Panama

## Contacts



**Michelle Martinelli**

Partner, Deloitte Legal Panama

[mmartinelli@deloitte.com](mailto:mmartinelli@deloitte.com)



**Juan Pablo Fábrega**

Senior Manager, Deloitte Legal Panama

[jufabrega@deloitte.com](mailto:jufabrega@deloitte.com)



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

## Updates in connection with data protection in the Republic of Panama

Law 81 of 2019 and Executive Decree 285 of 2021 (the DP Regulations) establishes the principles, obligations and procedures for data processing in Panama.

It is highly expected that the regulations are to be amended, specifically to include new data protection terms. Besides the regulations, the following general rules also govern data protection legislation:

- The constitution; and
- The criminal code.

## Main characteristics of the regulations

- They encompass the basic principles, rights, obligations and procedures applicable to the protection of personal data in Panama;
- Persons subject to the DP Regulations, such as natural or legal persons, private or public, as well as those entities that are classified as “regulated subjects” (i.e., banks, insurance companies, telecommunications providers, among others);
- Rights of the interested party to access, rectify, cancel, oppose and carry data; and
- Fines and penalties applicable to those who violate the rights to data protection of persons

## Sanctions

Depending on the seriousness of the breach, the following penalties can be imposed for breaching the DP Regulations:

- Minor offense: Required to appear before the relevant authority to provide information, records, or address alleged offenses;
- Serious misconduct: Fines proportionate to the offense; and
- Very serious misconduct:
  - Closure of database records and the corresponding fine; and
  - Suspension and temporary or permanent suspension of data processing activities, and the corresponding fine.

# ? What are the most relevant **cybersecurity updates**?

## Relevant cybersecurity updates

Panama aims to be a state that operates with an open, free, secure, and resilient cyberspace that safeguards the fundamental rights and freedoms of the Panamanian people, while allowing the government to serve its nationals and foster a regulatory environment favorable to the growth of the economy.

Panama was the second Latin American country, after the Dominican Republic, to ratify the Budapest Convention on Cybercrime, and as such, Law 79 of 2013 was promulgated.

In view of the fast evolution of information and communication technologies, an update in connection with security policies, criteria and recommendations to deal with new threats was required; as well as to counteract the possible impacts that may occur. In consequence, the Republic of Panama adopted Resolution 17 of 10 September 2021 (the Resolution), by means the National Cybersecurity Strategy for the period 2021-2024 entries into force.

The Resolution contains new guidelines, elements, measures, equipment duly updated and intends to control computer security applicable to public entities, as well as the carrying out of the necessary coordination for their corresponding use by the latter, and for the corresponding interaction of such measures with citizens and society in general.



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

## Relevant AI updates in Panama

A bill has been formally presented to the legislative authority for consideration, which will establish the legal framework, promotion and development of artificial intelligence (the AI Bill) in the Republic of Panama.

This initiative marks a significant step for the country in aligning with global jurisdictional standards. The main objective of the AI Bill, is to guarantee the protection of human rights, security and privacy of people, as well as to encourage innovation and technological development, ensuring that the use of the same, is ethical, safe and respectful of human rights and to be able to establish a national policy on AI.

The AI Bill is similar to the applicable law in the European Union (the EU AI Regulations), legislation that has already been approved, with many more nuances of restrictions and specific order.

The AI Bill, is meant to be applied to suppliers, implementers, importers and distributors of AI systems and models seeking to expand the capabilities of artificial intelligence.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Expected developments in data protection, cybersecurity and AI in Panama

In an increasingly digital business environment, cybersecurity is a strategic priority for Panamanian companies to protect their data and finances. With millions of cyberattack attempts recorded annually, it is essential for companies to adopt proactive and reactive measures to protect themselves against these tangible and intangible threats.

Some of the most important developments that can be expected are the following:

- Adoption of advanced security technologies;
- Constant updating of systems and applications;
- Cloud data protection and regular backups;
- Continuous monitoring and immediate response: detecting suspicious activities early on is critical to limit the impact of an attack;
- Fostering collaboration and the exchange of information on threats; and
- Implementing rigorous access controls



# Paraguay

## Contacts



**Daniel Fariña**

Partner, Deloitte Legal Paraguay  
dfarina@deloitte.com



**Victor Jara**

Senior Manager, Deloitte Legal Paraguay  
vjara@deloitte.com

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

## **Data protection and personal information in Paraguay**

Data protection and personal information in Paraguay began to be formally regulated by Law No. 1682/01, amendments, Law No. 1969/02 and Law No. 5543/15, which in summary prohibited the illegal disclosure or dissemination of personal or sensitive data for credit purposes.

In October 2020, Law No. 6534/20 “On the Protection of Personal Credit Data” came into force, repealing Law No. 1682/01 and its amendments. This new law establishes the protection of data and personal information in Paraguay, with two enforcement authorities, the Central Bank of Paraguay (BCP) and the Secretariat for the Defense of Consumers and Users (SEDECO), authorities in charge of sanctioning breaches of said law.

Law No. 6534/20 guarantees the protection of credit data of all persons, whether Paraguayan or foreign. Likewise, the activity of collecting and accessing credit information data is regulated. The application of this law is mandatory for the processing of personal data in public or private records collected or stored in Paraguayan territory in information systems, physical, electronic or similar databases.

To understand the concepts according to this law:

- Personal data: Information of any type, referring to legal persons or specific or identifiable natural persons;
- Sensitive personal data: Those that refer to the intimate sphere of its owner, or whose improper use may give rise to discrimination or entail a serious risk for the latter, such as racial or ethnic origin, religious, philosophical and moral beliefs, convictions, genetic data or biometric data, etc.; and

- Credit information: Understood as information, positive and negative, that is related to the credit history of natural and legal persons, about credit, commercial and other activities of a similar nature, which serves to correctly and unequivocally identify the person.

## **Violations of the law**

The Central Bank of Paraguay and the Consumer and User Defense Secretariat shall be competent, each within their area of competence, to sanction administrative violations of this Law and its regulations.

The following shall be considered violations:

- The exercise of activities established in this law, without the prior authorization of the Central Bank of Paraguay;
- The exercise of activities not contained in the authorization to operate or in the social statutes;
- Collecting personal data for use in a database without providing sufficient and ample information to the interested party, in accordance with the technical specifications established in the regulations for the application of this law;
- Omitting mandatory information or providing incomplete or false information to the Information Center of the Superintendency of Banks of the Central Bank of Paraguay; and
- Omitting mandatory information or providing totally or partially false information to the Central Bank of Paraguay, among others.

## Sanctions contemplated by the law

The control authority may impose the following sanctions on those responsible for and in charge of the treatment:

- Warning, admonition;
- Fine of up to 15,000 minimum daily wages in force at the time of the imposition of the sanction;
- In the event of a repeat offence of the same infringement, the fine will be double the initial fine applied, which may be increased up to 50,000 minimum daily wages in force at the time of the imposition of the sanction for the natural or legal person who registers an annual turnover of more than PYG 6 billion (approx. US\$790,000);
- Suspension of activities related to data processing for up to a period of six months, the corrective measures to be adopted will be indicated in the act of suspension;
- Disqualification from holding a job, position or commission within the financial and credit system and in personal data information companies, for a period of six months to five years;
- Temporary closure of operations related to data processing once the suspension period has elapsed without the corrective measures ordered by the control authority having been adopted; and
- Immediate and definitive closure of the operation involving the processing of sensitive data.

## Duty of confidentiality

The persons responsible for, in charge of, the processing of credit data and those involved in any phase of the collection, processing, storage, use or circulation of data for credit purposes are obliged to maintain confidentiality regarding the same, unless it is required to be revealed by a competent authority through a court order.

The duty of confidentiality is maintained even when the person responsible ceases their duties.

This obligation is extensible to persons duly recognized as users or subscribers of a credit information company, who have access, in accordance with the provisions of the law, to the data history of a holder; as they must maintain absolute confidentiality and care regarding the information obtained.

## Consent

Law No. 6534/20 guarantees that every person will be informed in an express and clear manner of the purpose for which the personal data requested about them will be used, so that they can expressly express their consent for the collection and use of their personal data. Such consent must be express and unequivocal, in writing, electronically, digitally or by another reliable mechanism. Consent may be expressly revoked under the same conditions, free of charge, without retroactive effect.

## Period of conservation of information

This law provides that credit information may be published for a maximum period of five years, counting from the last significant information, or from the expiration of the original term of the credit operation in question, whichever is greater.

# ? What are the most relevant **cybersecurity updates**?

## National Cybersecurity Plan of Paraguay

Paraguay has a National Cybersecurity Plan, approved by Decree No. 7,052/17, after a process of several years that involved representatives of more than 120 organizations, both public and private institutions, professional associations, international organizations, among others.

This plan arose from the need to strengthen activities related to cybersecurity and information protection, not only in terms of incident response capacity, but also in terms of training and awareness, protection of critical infrastructure, security in public administration, research capacity, etc.

Law No. 6207/18 created the Ministry of Research and Communication Technologies (MITIC), which, thanks to this ministry and through the General Directorate of Cybersecurity and Information Protection, continues to be watched over and strengthened the cybersecurity and information protection, with powers according to the scenarios faced.

## Responsibilities

This plan has the following responsibilities:

- Implement mechanisms for management, coordination, response and investigation of cyber incidents that put the national digital ecosystem at risk;
- Establish and encourage mechanisms for the exchange of information related to cyber incidents and threats, between the government, private, regional and international sectors;
- Implement mechanisms and develop activities leading to the protection of systems, networks, processes and information of state agencies and entities, as well as critical technological infrastructures, with a preventive approach;
- Promote awareness initiatives and training plans on cybersecurity and information protection, in coordination with public institutions, the private sector, educational institutions and international organizations;
- Establish, manage and promote the adoption of policies, standards, guidelines, guides and information protection frameworks for state agencies and entities;
- Propose and promote the adoption of good practice guides for cybersecurity and information protection throughout the national ecosystem; and
- Propose, coordinate, manage and monitor cybersecurity plans and strategies at the national level.



## The CERT-PY - National Cyber Incident Response Center

Dependent on the General Directorate of Cybersecurity and Information Protection of the Ministry of Information and Communication Technologies (MITIC), its main objective is to act as a central coordinator for notifications of security incidents in Paraguay, providing the necessary support to respond to these incidents, acting as a coordinator between the affected and involved parties for their resolution.

Its main functions include:

- Implement mechanisms for management, coordination, response and investigation of cyber incidents that put the national digital ecosystem at risk;
- Implement and promote mechanisms for monitoring and detecting cyber incidents in state agencies and entities, as well as in national critical infrastructures;
- Establish and encourage mechanisms for exchanging information related to cyber incidents and threats between the government, private, regional and international sectors;
- Implement mechanisms and develop activities for the generation, collection, processing and analysis of cybersecurity information among actors in the ecosystem; and
- Implement and promote early warning mechanisms for incidents and threats.



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

## The regulation of AI in Paraguay

Currently in Paraguay, the legislative power indicated that the objective of the current normative progress and criteria is to obtain multi-sectoral positions that allow the construction of legislative proposals and spaces for debate on the use and implementation of artificial intelligence in Paraguay.

Omitting actions now could mean missing out on the future benefits that artificial intelligence offers for national development.

First world countries are discussing how to legislate on the use and implementation of this technology.

The Vice Minister of the Ministry of Information and Communications Technologies (MITIC), in a statement, recalls that data protection is a fundamental aspect in this matter. Likewise, there are areas of the public sector that need technological tools to improve their internal management, but that these tools require non-accessible data, which makes their development impossible.

Existing external tools could be used to enhance various projects, but it is necessary to develop the tools to guarantee the appropriate use and protection of private data.

In October 2023, the draft law to legislate artificial intelligence in Paraguay was being reviewed in a public hearing, which is still in process.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Data protection, cybersecurity and AI in Paraguay

### Paraguay in development

In Paraguay, although no significant progress in the areas of data protection, cybersecurity, and artificial intelligence has been made, leveraging all necessary tools and resources ensures efficient data and information safeguarding in full compliance with relevant regulations.

Currently, Paraguay is in the early stages of developing a robust framework for data protection and cybersecurity. Despite the lack of comprehensive legislation in these areas, there is a growing awareness of their importance among both the public and private sectors.

Organizations are beginning to recognize the critical need for protecting sensitive information and are taking initial steps to implement basic security measures.

In terms of artificial intelligence, Paraguay is still exploring the potential benefits and applications of this technology. While there are few AI initiatives currently in place, the government and various institutions are showing interest in fostering innovation and research in this field. The aim is to create an environment where AI can be developed and utilized responsibly, ensuring that it aligns with ethical standards and contributes positively to societal advancement.

Looking ahead, it is crucial for Paraguay to establish a comprehensive regulatory framework that addresses the challenges and opportunities presented by data protection, cybersecurity, and AI. By doing so, the country can ensure that it is well-equipped to handle the complexities of the digital age, protect its citizens' data, and harness the power of AI for sustainable development.

### Paraguay in the near future

Looking forward, it is expected that data protection, cybersecurity, and AI in Paraguay will evolve to meet the highest international standards. Comprehensive regulations are anticipated, aiming to safeguard sensitive information and foster a secure digital environment. This will involve collaboration between the government, private sector, and academic institutions to create robust policies and implement cutting-edge technologies. By doing so, this fosters trust among citizens and businesses by ensuring their data is handled with utmost care and security.

Furthermore, it is expected that AI will play a transformative role in various sectors within Paraguay, from healthcare and education to finance and agriculture. The responsible and ethical use of AI has the potential to drive innovation and efficiency, addressing some of the country's most pressing challenges. By investing in AI research and development and ensuring that it is integrated with strong data protection and cybersecurity measures, Paraguay can pave the way for a more prosperous and technologically advanced future.

# Peru

## Contacts



**Jose Francisco Iturrizaga**

Partner, Deloitte Legal Peru

[jiturrizaga@deloitte.com](mailto:jiturrizaga@deloitte.com)



**Mariana Cordero**

Senior Lawyer, Deloitte Legal Peru

[marcordero@deloitte.com](mailto:marcordero@deloitte.com)



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

## **Ministry of Justice and Human Rights (MINJUSDH) supervises the collection of Personal Data**

On 8 May 2024, the company Tools for Humanity Corporation (TFH) began its activities in Peru with a project performing facial and iris scans of interested individuals to generate a unique global identity, in exchange for access to cryptocurrencies called Worldcoin.

On 13 May 2024, the Directorate of Supervision and Instruction of the National Authority for the Protection of Personal Data (ANPD) of the [MINJUSDH initiated supervisory actions to determine whether the data processing conducted by this company complies](#) with the provisions of Law No. 29733, the Personal Data Protection Law, and its regulations.

Their processing system relies on a device known as the “Orb”, which synchronizes with the person’s phone, who previously booked an appointment through an application. The Orb scans the iris of the eye and provides a unique code that presumably no one else possesses.

The ANPD recommends that citizens demand and read privacy policies, in which the intended use of the collected data, the entity responsible for processing, where the data will be stored, with whom it will be shared and the consequences of providing the data should be disclosed.

To date, the ANPD has not announced the results of its investigations and the actions that may be taken if a violation of the Personal Data Protection Law is determined.

## **MINJUSDH imposed sanctions on companies for obstructing supervision of compliance with the Personal Data Protections Law and its regulations**

The MINJUSDH, through the National Authority for the Protection of Personal Data (ANPD), [sanctioned a telecommunications company for repeatedly failing to respond to information requests made by the ANPD](#), constituting an infringement for obstructing the supervisory function. The requests aimed to investigate an alleged improper processing of a complainant’s personal data, which was affected by incorrect identity validation allowing a third party to acquire a phone line in the complainant’s name and withdraw a considerable amount of money from their credit card. The sanction was confirmed on appeal in 2024 with a fine of 22.50 UIT (US\$30,900).

Additionally, this same company was previously sanctioned for obstructing the ANPD’s supervisory function by not providing the required information to investigate potential personal data violations of another complainant. This violation occurred due to incorrect identity validation, allowing a third party to improperly acquire a phone line in the complainant’s name and conduct multiple unauthorized financial operations, such as withdrawals, services payments, among others, with the complainant’s debit and credit cards. This sanction was also confirmed on appeal in 2024 with a fine of 19.13 UIT (US\$26,272).

It is pertinent to highlight that data controllers and processors have a legal duty to cooperate and provide all necessary facilities for authorities to execute their supervisory powers.

# ? What are the most relevant **cybersecurity updates?**

## **Cybercrime in Peru: [State strategies and challenges report](#)**

**Published May 2023**

The Peruvian Ombudsman's Office is an autonomous constitutional organization in charge of protecting the constitutional rights and freedoms of the individual and the community, monitor the performance of the duties of the state administration, and the provision of public services to the population.

While legislation is essential for enabling a series of actions to combat cybercrime, the progress and effectiveness of these actions depend on various factors, including the commitment of the state to foster public policies and provide the necessary resources to strengthen the capacities and duties of the main operators of the justice administration. There should be a coordinated work for the prevention, prosecution and control of cybercrimes between the National Police, the Public Prosecutor's Office and the Judiciary.

While the advantages of information and communication technologies are undeniable, the increased use of the internet in recent years has created a scenario that is exploited by cybercrime, affecting vulnerable populations such as children, adolescents, and the elderly, exacerbated by the lack of knowledge some people have about managing and safeguarding personal data.

Reports of cybercrimes filed with the National Police quadrupled between 2018 and 2021, with the most recurrent being computer fraud and identity theft. There is also a significant increase in recent years in investigations of cybercrimes against the sexual indemnity of children and the sexual freedom of adolescents, handled by the police's criminal investigation departments.

Also, the Divindat–PNP (Division of High Technology Crimes of the National Police) has developed informational materials on the risks of unsafe use of information and communication technologies and on the different types of cybercrimes. This information is published on the National Police's web portal and in person at various awareness-raising activities, aimed at the general population to enhance public understanding of cyberthreats and promote safe online practices.

The Specialized Cybercrime Prosecutor's Unit has established a significant strategic alliance with the UNODC's Global Programme on Cybercrime enabling the organization, in coordination with the Public Prosecutor's Office School, of basic and specialized courses on cybercrime for its entire staff, the staff of the Corporate Specialized Cybercrime Prosecutor's Office of Central Lima, and members of the network of prosecutors nationwide. This inter-institutional strategy also facilitated the development of 14 training modules on topics such as investigative methods in cybercrime, digital forensic analysis, international judicial cooperation, and related subjects. levels.

The Ombudsman's Office has been promoting various training activities aimed at improving the protection of the rights of vulnerable populations against the new criminal modalities arising from access to social networks and other digital media. In November 2021, it launched a campaign called “Únete contra el cibercrimin” (Join against cybercrime), with the goal of raising awareness and alerting about these new forms of crime and informing the public about the mechanisms for reporting them to the competent authorities.



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

## **Promoting the use of AI in favor of the country's economic and social development**

On 5 July 2023, Law No. 31814 was published, [a law that promotes the use of artificial intelligence in favor of the country's economic and social development](#), with the aim of fostering digital transformation in a secure environment that guarantees its ethical, sustainable, transparent, replicable, and responsible use.

The law declares that it is of national interest to promote digital talent in the utilization of emerging and new technologies in favor of social and economic well-being, as well as to encourage the development and use of artificial intelligence to improve public services, education and learning, health, justice, public safety, digital security, the economy, inclusion, social programs, national security and defense, as well as any other economic and social activity at the national level.

Additionally, the law establishes a series of principles for the development and use of artificial intelligence and indicates that the Presidency of the Council of Ministers, through the Secretariat of Government and Digital Transformation, is the technical-normative authority responsible for directing, evaluating, and supervising the use and promotion of the development of artificial intelligence and emerging technologies. This authority must submit an annual report to the Congress of the Republic on the progress in the implementation of the National Digital Transformation Policy and the National Artificial Intelligence Strategy.

## **New draft regulation promoting the use of AI in favor of the country's economic and social development**

On November 19, 2024, the new draft regulation of Law No. 31814, [the law that promotes the use of artificial intelligence for the economic and social development of the country](#), was published.

The draft regulation develops a series of key aspects, and the following provisions stand out:

- A criteria for classifying AI-based systems into those of unacceptable risk and high risk are detailed, according to the risk-based approach adopted by the AI Law.
- The proposed National AI Authority is the Presidency of the Council of Ministers, through the Secretariat of Government and Digital Transformation.
- Security measures to be adopted by those using AI software, including data encryption, anomaly detection, model robustness, privacy by design, security audits and education and awareness.
- The inclusion of new definitions such as “Digital Citizenship”, “Digital Infrastructure”, “AI Privacy”, among others, to provide clarity in the application of the Law and its regulation.



- Public-private collaboration: The regulation encourages collaboration between the public and private sectors to drive AI innovation and application, promoting partnerships and shared resources.
- Monitoring and evaluation: Mechanisms for the continuous monitoring and evaluation of AI systems are established to ensure compliance with the regulation and to adapt to emerging challenges and opportunities.

## **Progressive implementation of AI use in Peruvian consular offices is approved**

On 30 May 2024, the Plenary of Congress approved, by majority, the legislative proposal that guarantees the [progressive implementation of digital transformation in Peru's consular offices](#) abroad, with 97 votes in favor, one against and one abstention.

Bills 6852/2023 and 7619/2023 promote the use of emerging technologies such as AI to provide efficient, transparent and timely public services to citizens residing in Peru and abroad. This would represent an effort by the Ministry of Foreign Affairs to gradually and progressively improve consular services through the use of technologies in consular offices, aspiring to achieve an ideal situation in terms of accessibility, speed, and efficiency of the state's consular services for Peruvians abroad.

This proposed law would seamlessly integrate into the national regulatory system because it aligns with Legislative Decree No. 1412 – Digital Government Law, and Law No. 31814, which promoted the use of AI for the country's economic and social development.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## **New regulation of the Law No. 29733 on the Personal Data Protection Law will come into effect March 30, 2025.**

### **[Supreme Decree No. 016-2024-JUS](#)**

On November 30, 2024, the Supreme Decree No. 016-2024-JUS approving the new regulation of the Law No. 29733 was published and will come into effect on March 30, 2025.

The main regulatory changes are: (i) the extra-territorial application of the Law and its regulation to data bank holders or data controllers who are not located in Peruvian territory but engage in activities related to the offering of goods or services directed at data subjects located in Peruvian territory and activities aimed at analyzing the behavior of data subjects located in Peruvian territory; (ii) mandatory designation of a data processing representative in Peru; (iii) measures for the processing of personal data of children and adolescents; (iv) obtention of consent for advertising purposes; (v) notification of security incidents to the Authority and the affected data subject; (vi) the designation of a personal data compliance officer when large volumes of personal data is processed and/or they process sensitive data as a primary or core business; (vii) the right to data portability; (viii) mitigating factors of liability in an administrative sanction procedure; and, (ix) the creation of the digital platform “Yo Cuido Mis Datos Personales” (“I Take Care Of My Personal Data”) to facilitate the filing of complaints of personal data holders regarding violation of their rights.

## **New bill projects to regulate AI**

To date, legislators continue to present initiatives focused on regulating AI to prevent crimes and apply it in specific sectors, such as the administration of justice, public safety, and transportation.

Law No. 31814 and the National Digital Transformation Policy promote the use of this technology, which is something that must be maintained in these new initiatives. Nevertheless, the bill projects don't correlate with the approved norms and establish measures that would discourage the use of AI, stemming from a negative conception of AI proposing to strictly regulate it.

An example of this is [Bill No. 7033/2023-CR](#) which proposes to impose responsibilities on AI system developers and providers for the misuse of this technology, obliging them to repair the damages caused and compensate the affected individuals. This could discourage the incorporation of emerging technologies due to the possible consequences imposed by the regulatory framework.

Also, some project create regulatory duplicity with what is stipulated in Law No. 31814, which could cause confusion and additional burdens for those in the AI sector, having to comply with multiple similar regulations.

Legislators must carefully evaluate the need for new provisions to avoid falling into overregulation and ensure that the measures adopted undergo a proportionality analysis. Adding strict regulations could negatively impact the country's innovative development.

# Poland

## Contacts



**Monika Skocz**

Local Partner, Deloitte Legal Poland  
[mskocz@deloittece.com](mailto:mskocz@deloittece.com)



**Michał Mostowik**

Senior Managing Associate, Deloitte Legal Poland  
[mmostowik@deloittece.com](mailto:mmostowik@deloittece.com)

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

## **Data protection in New Electronic Communications Law**

November 2024 will see the introduction of the new Electronic Communications Law (ECL), which will not go without a profound effect on the personal data protection area. Here are the most important changes.

### **One marketing consent**

The ECL consolidates regulations for obtaining consent for sending commercial and marketing information by introducing a single marketing consent under Article 398. This replaces the previous provisions in the Telecommunications Act and Article 10 of the Act on the Provision of Electronic Services. It should finally resolve the discussion that was in place under previous law and reassure the business organizations that when engaging in direct marketing they will need to obtain only one type of consent for one type of direct marketing action that would be in line with the ECL. Under previous regulations there were voices demanding obtaining two types of consents for each type of action fulfilling criteria set forth in the two regulations that are being replaced by the ECL.

### **Record keeping**

Electronic communication providers will be required to maintain a record of personal data breaches, documenting their circumstances and the actions taken in response to these breaches.

### **Confidentiality and security**

Electronic communication providers will be also required to uphold the confidentiality of communications and secure telecommunications equipment and data (Article 387 ECL).

They will have to inform end-users about the processing of transmission data, their options for influencing this processing, and the types of data used for marketing purposes (Article 391 ECL).

## **New obligations related to the protection of minors**

In the light of the new rules implemented in the Polish legislative system in August 2024, concerning the protection of minors, specified employers (generally those whose activities involve working with children or where children are or may be present) shall have several new obligations, including:

- Verify employees and other individuals employed in the sexual offenders' registry; and
- Establish standards for the protection of minors.

Entities providing hotel and tourism services, as well as those operating other collective accommodation facilities, also have the obligation to implement standards to ensure the protection of minors.

This will increase the volume of personal data processed by these entities. Polish data protection authority emphasized the need to maintain personal data protection standards in these processes. In particular, personal data controllers should pay attention to the following:

- Conducting a risk analysis for processing personal data, verifying data protection policies and reviewing methods of implementing the GDPR obligations; and
- Adapting existing solutions that take into consideration data protection by design and by default, ensuring that methods for processing data comply with the new legal standards.





## Data protection in Whistleblower Protection Act

In June 2024, Poland implemented the EU Whistleblowing Directive through Whistleblower Protection Act. The new legislation came into force on 25 September 2024. The new regulations impose several new obligations on business organizations including duties related to protection of personal data of involved parties.

### Prohibition of disclosure of whistleblower data

The act indicates that the whistleblowers' personal data allowing their identity to be determined are not subject to disclosure to unauthorized persons, unless with the express consent of the whistleblower (with exception to situations where the disclosure of identity is necessary and proportionate in connection with an investigation or investigation by public authorities or in order to guarantee the rights of defense of the person concerned).

### The principle of data minimization

The new regulation emphasizes the application of data minimization rule. Personal data that is not relevant to the processing is not to be collected. In cases of accidental collection, such data is immediately deleted and must be erased within 14 days of determining its irrelevance.

### Obligations related to internal documentation regarding data protection

The data controllers setting up the whistleblowing system will be required to:

- Adapt the record of processing activities; and
- Carry out a data protection impact assessment (DPIA) for whistleblowing system.

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 and regulate the relationship with any external provider.

### Information obligation

The act reinforces that the information obligation needs to be carried out in respect to:

- The whistleblower;
- The person accused of the violation; and
- Other individuals with knowledge of the violation (witnesses or victims).

It is important to note that the controller is exempt from the obligation to inform about the source of the data – both when the controller fulfills the information obligation resulting from GDPR and also when the person whose data is processed exercises their right to access personal data processed by the controller.

### Data retention

Data related to submission of 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 three years following the end of the calendar year in which the follow-up action was completed or the proceedings initiated by that action.



## Most notable Data Protection Authority decisions in Poland

### Polish Data Protection Authority fined a bank PLN 4 million for failure to notify the victims of a data leak

The Polish Data Protection Authority (UODO) has imposed a fine of PLN 4,053,173 (€928,498.06) on a bank for violating several provisions of the General Data Protection Regulation (GDPR). The fine stems from a data breach incident where an employee of a third-party processor mistakenly sent sensitive client documents, including personal identification numbers, financial data, and account information, to another bank.

Despite the other bank returning the documents, the UODO determined that the bank failed to adequately assess the risks associated with the breach, which posed a significant threat to clients' rights and freedoms, such as potential identity theft and banking fraud.

**The UODO emphasized that the mere status of the other bank as a business partner did not automatically classify it as a "trusted party."** As a result, UODO mandated that bank should notify the affected data subjects about the breach and its implications, reinforcing the importance of compliance with GDPR obligations in data protection.

### Administrative fine of PLN 100,000 for failure to notify a personal data breach

The President of UODO has imposed an administrative fine in the amount of PLN 103,752 (€24,000) on an insurance company. The personal data breach involved only one individual who did not suffer any harm. The reason for imposing the administrative fine was a failure to notify the affected individual of the personal data breach.

The decision showed that UODO adopted a strict approach towards assessment of requirement to communicate the data breach to data subject and that the data protection authority does not rely on risk assessments carried out by data controllers in that respect. UODO assesses the risk connected with data breach independently. The outcome of UODO assessment may be less favorable for the controller, so when deciding not to inform a data subject about a data breach, the controller should be confident that the risk connected with the incident was indeed low.

### Fine of almost PLN 1.5 million for a medical company after hacker attack

The UODO has imposed a fine of PLN 1,440,549 (€330,000) on a medical company for failing to protect personal data. The hackers got access to company's network drives with personal data of about 21,000 company's employees and patients and installed a ransomware software. In the view of UODO in the assessed situation the controller did not implement appropriate technical and organizational measures under Article 32 GDPR.

## Bank fined PLN 1.4 million for a personal data breach

On 2 April 2024, the UODO imposed an administrative fine of PLN 1.4 million (approx. €360,080) on a bank.

UODO learned about the personal data breach at bank from the media. It transpired that some sensitive bank documents were found abandoned in a public place, after they had been stolen from a courier company. The data controller did not report the breach, citing the quick recovery and fact, that the person who found the documents took them directly to the police station and stated that he had not copied the documents found. UODO questioned this decision, emphasizing the following:

- The risk of violating rights or freedoms in the event of a data breach should be assessed from the perspective of the affected individual, not the interests of the data controller.
- Failure to notify individuals about the breach, especially in cases of high risk, deprives them of the ability to respond and assess the potential consequences.
- Not reporting the breach to UODO prevents the authority from assessing the risk and verifying if the controller took adequate measures to address the breach and prevent future occurrences.
- It doesn't matter that only one identified person found the documents. The uncertainty about how many others might have accessed the data beforehand makes the breach significant.

# ? What are the most relevant **cybersecurity updates**?

## **A new version of the draft law implementing the NIS2 Directive**

On 7 October 2024, as part of the conference of the Minister of Digital Affairs, a new draft of the act implementing the NIS2 Directive into the Polish legal system was presented (draft of 3 October 2024).

The implementation of the NIS2 Directive will be carried out through an amendment to the Act on the National Cybersecurity System. This is the second draft of the implementing act, which considers the conclusions resulting from the public consultations. The consultations met with great interest from the market, during which more than 1,500 comments were submitted.

Most comments submitted during the consultation process focused on clarifying and refining the scope and definitions within the proposed amendments. Stakeholders raised concerns about the potential overlap between the new regulations and existing legal frameworks, particularly in relation to the telecommunications sector. There were numerous requests for more precise definitions of key terms, such as "essential entities" and "important entities," to ensure proper classification of organizations subject to new requirements. Additionally, many commenters sought clarification on the specific obligations that would be imposed on different types of entities, emphasizing the need for proportionality in relation to the size and risk profile of each organization.

Another significant area of concern was the implementation timeline and the potential burden on businesses, especially small and medium-sized enterprises (SMEs). Many stakeholders requested longer transition periods to allow for adequate preparation and implementation of the new cybersecurity measures.

Furthermore, several comments addressed the need for more detailed guidance on risk assessment methodologies and minimum-security requirements, as well as calls for greater alignment with existing EU regulations and international standards to avoid conflicting obligations and unnecessary complexity in compliance efforts.

The most important changes resulting from the draft law of 3 October 2024 implementing NIS2 Directive, in comparison to the draft law of 3 April 2024 include:

- The list of entities subject to regulation has been extended and the rules for identifying key entities have been partially changed. Changes have also been made to some definitions;
- Manufacturing sectors (including chemicals and food production) have been identified as important rather than critical sectors;
- The requirements for supply chain security will relate only to direct suppliers;
- The deadline for the first cybersecurity audit has been extended from 12 to 24 months;
- The provisions relating to ISO standards, the fulfilment of which introduced a presumption of compliance with certain requirements resulting from the draft law, were deleted;
- Changes have been made to the functioning of the register of critical and important entities;
- The decision to recognize as a high-risk supplier will also include entities from the capital group of a given supplier; and
- The catalogue of cases in which fines can be imposed has been extended.

## New law for the implementation of DORA into Polish law

In October 2024, a second draft act on the amendment of certain acts in connection with ensuring the operational digital resilience of the financial sector and issuing European green bonds was published. This draft implements and ensures the application of the Digital Operational Resilience Act (DORA) and the accompanying 2022/2556 directive into Polish law, as well as – in comparison to the initially published version of the draft – European Green Bonds Regulation.

The DORA regulation will generally apply directly to financial entities and does not require implementation into Polish law. However, certain provisions necessitate adjustments to the Polish legal framework, particularly in designating competent authorities and imposing obligations on financial entities. As a result, the Ministry of Finance published the draft, amending laws such as the Banking Law, the Payment Services Act, and the Act on Trading in Financial Instruments. These amendments are mainly technical and aim to align national law with DORA's provisions. DORA allows for the exclusion of certain entities (in Poland, credit unions and the Bank Gospodarstwa Krajowego (BGK)) from the scope of the new regulations. However, the Polish legislator opted for uniform application of the rules across financial entities. Moreover, in the case of BGK, the legislator decided to expand the scope of obligations beyond those required by DORA, imposing on BGK the requirement to apply all obligations related to ICT risk management. Additionally, the draft provides for, among others:

- The designation of the Polish Financial Supervision Authority (KNF) as the body responsible for supervising compliance with the DORA regulation, along with granting it several supervisory powers; and
- The timelines and rules for financial entities to submit information and reports regarding the DORA regulation to the KNF.

The new law is expected to come into force on 17 January 2025, with a few exceptions that will apply the day after its announcement, alongside the application of the DORA regulation. Since the draft has not yet been adopted, further modifications may still occur.

## KNF's self-assessment survey

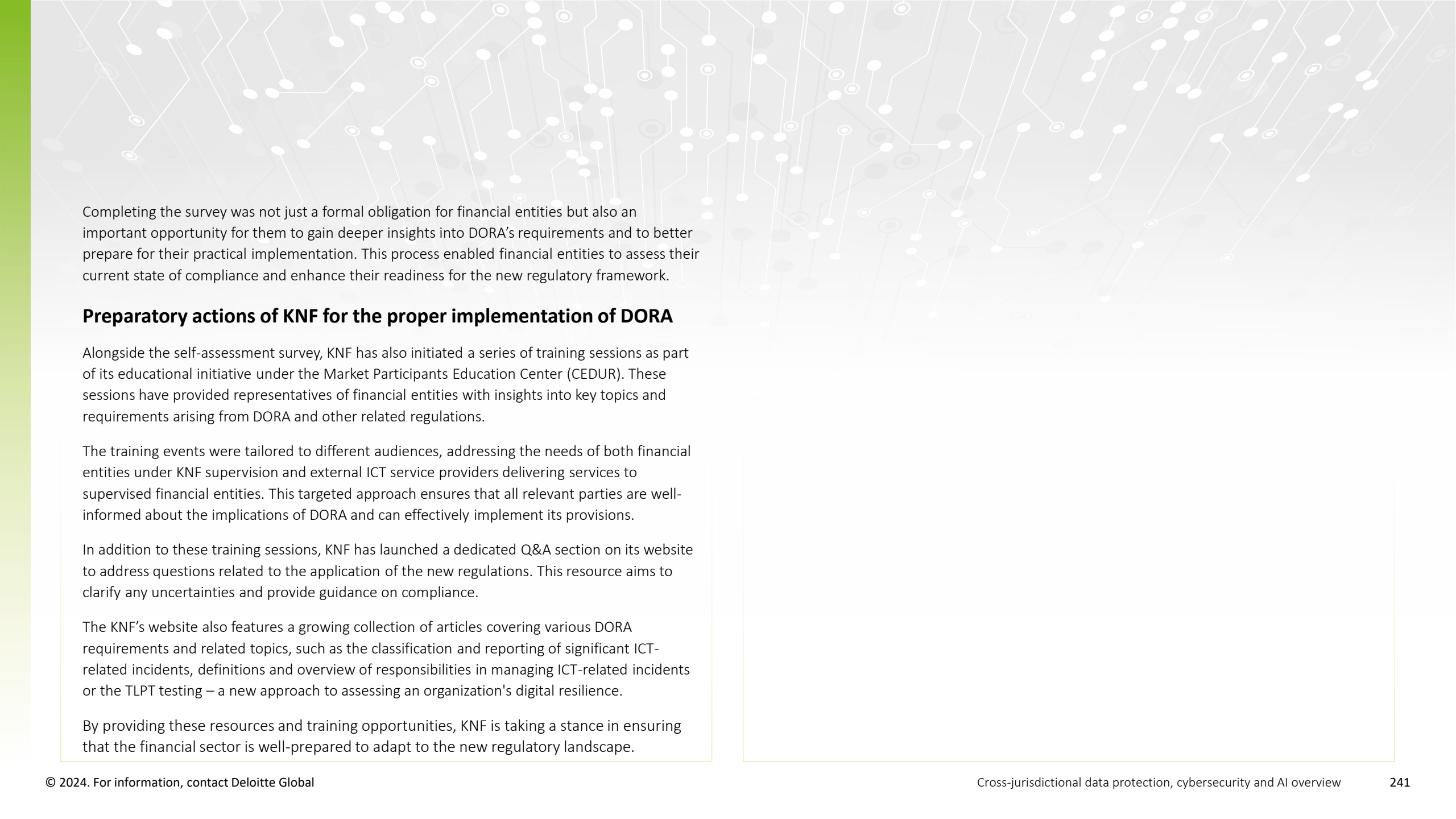
The KNF has taken a proactive and comprehensive approach to prepare for the implementation of the DORA regulation. One of the cornerstone initiatives in these efforts has been the development of a self-assessment survey aimed at gathering both quantitative and qualitative data to measure how well financial entities are aligning with DORA's requirements. Through this detailed survey, KNF can assess the readiness of financial entities to effectively manage technology-related risks, ensuring they are better equipped for the forthcoming regulatory changes.

The survey, consisting of 200 points, reflects the specific requirements detailed in the regulation, addressing primarily the requirements outlined in Articles 5-30 and in Article 45 of DORA. Each section features the exact wording of the requirement, the corresponding subsection text, and space for financial entities to describe their compliance status (including assessment regarding the level of requirement fulfillment).

It also introduces key definitions to assist respondents in categorizing their status, such as:

- Business size categories (micro, small, medium, and large enterprises);
- Methods of requirement implementation (automatically, semi-automatically, or manually); and
- Levels of compliance (full compliance, partial compliance, non-compliance, or not applicable).





Completing the survey was not just a formal obligation for financial entities but also an important opportunity for them to gain deeper insights into DORA's requirements and to better prepare for their practical implementation. This process enabled financial entities to assess their current state of compliance and enhance their readiness for the new regulatory framework.

## **Preparatory actions of KNF for the proper implementation of DORA**

Alongside the self-assessment survey, KNF has also initiated a series of training sessions as part of its educational initiative under the Market Participants Education Center (CEDUR). These sessions have provided representatives of financial entities with insights into key topics and requirements arising from DORA and other related regulations.

The training events were tailored to different audiences, addressing the needs of both financial entities under KNF supervision and external ICT service providers delivering services to supervised financial entities. This targeted approach ensures that all relevant parties are well-informed about the implications of DORA and can effectively implement its provisions.

In addition to these training sessions, KNF has launched a dedicated Q&A section on its website to address questions related to the application of the new regulations. This resource aims to clarify any uncertainties and provide guidance on compliance.

The KNF's website also features a growing collection of articles covering various DORA requirements and related topics, such as the classification and reporting of significant ICT-related incidents, definitions and overview of responsibilities in managing ICT-related incidents or the TLPT testing – a new approach to assessing an organization's digital resilience.

By providing these resources and training opportunities, KNF is taking a stance in ensuring that the financial sector is well-prepared to adapt to the new regulatory landscape.



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

## **The draft law on AI systems and a new AI Commission**

On 16 October 2024, a long-awaited draft law on AI systems was published, aimed at implementing the AI Act in Poland. This date also marks the start of public consultations on how the AI Act should be applied in the country (stakeholders have 30 days to express their views).

A key feature of the draft is the proposal to establish a new regulatory body: the Commission for the Development and Security of AI. This commission will act as the market surveillance authority under the AI Act and will be composed of a president and nine members, representing two government ministries and seven other public institutions, including the Personal Data Protection Office, the Office for Competition and Consumer Protection, the Financial Supervision Authority, the Ombudsman, the Ombudsman for Children, the National Broadcasting Council, and the Electronic Communication Office. Additionally, the commission will collaborate with other entities, such as the Financial Ombudsman and the Polish Patent Office. The aim of such move is to ensure a comprehensive and interdisciplinary supervision of AI systems.

The commission will have extensive oversight powers, including the authority to initiate proceedings, access files, documents and correspondence, as well as access IT systems and devices. It will also be empowered to issue explanations, opinions, and interpretations that hold significant importance for the application of AI regulations, including the capacity to provide individual interpretations similar to those in tax law. Furthermore, the commission will be responsible for establishing regulatory sandboxes to foster innovation in AI.

Appeals against the commission's decisions will be handled by the Competition and Consumer Protection Court. This approach allows for both formal and substantive assessments of the decisions made, ensuring comprehensive judicial oversight, akin to the judicial framework for competition and consumer protection or infrastructure sectors regulations (e.g., energy, telecommunication), yet in contrast to personal data matters.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Polish Supervisory Authority initiated an investigation into OpenAI

The Polish Supervisory Authority (UODO) is investigating a complaint about ChatGPT, in which the complainant accuses OpenAI, the tool's creator, of unlawfully and untrustworthy processing data, with unclear rules governing this process.

The allegations raised in the complaint raise concerns about OpenAI's systematic approach to European data protection principles. The UODO will therefore seek to clarify these doubts, particularly in light of the fundamental principle of privacy by design outlined in the GDPR.

## Revision of the UODO guides

Updates on the following UODO guides are expected to be finalized soon:

- The 2018 guide on data processing in recruitment: *Data Protection in the Workplace. A guide for employers*; and
- The 2019 guide on responding to personal data breaches: *How controllers should deal with data protection breaches*.

## New guidelines on personal data processing by trade unions

Mirosław Wróblewski, the President of the Polish Supervisory Authority, announced the creation of a separate guide on personal data protection dedicated to trade unions. The details are not yet known.

# Portugal

## Contacts



**Jacinto Moniz de Bettencourt**

Partner, Deloitte Legal Portugal

[jbettencourt@deloitte.pt](mailto:jbettencourt@deloitte.pt)



**Joana Diniz de Figueiredo**

Managing Associate, Deloitte Legal Portugal

[joanafigueiredo@deloitte.pt](mailto:joanafigueiredo@deloitte.pt)



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

## **Portugal's Data Protection Authority (CNPD) orders the temporary suspension of biometric data collection by a cryptocurrency company**

The CNPD issued Deliberation 2024/137, ordering this urgent measure, enacted for 90 days, after numerous complaints that biometric data such as iris, eye, and face scans were being collected on a large scale without proper consent or safeguards, including the involvement of minors without parental authorization. The purposes of such collection included the creation of a “digital identity proof”.

Additionally, issues were raised about the lack of clear information, the inability to delete data, and the absence of an age verification mechanism. Over 300,000 individuals had already participated, lured by the promise of cryptocurrency rewards, even though they were given little to no information regarding the processing operations carried out by the device.

CNPD's intervention reflects concerns over the heightened risks associated with processing biometric data, a special category under the GDPR, and emphasizes the need for robust protection, especially for vulnerable groups like minors.

CNPD found that:

- The information on the processing of biometric data provided to data subjects is insufficient and inadequate;
- The purposes of processing are not properly defined; and
- No information is provided to data subjects on withdrawing consent.

As a result, the CNPD ordered the temporary restriction of the processing of biometric data under the terms and for the purposes established.

## **Legal opinion on the creation of a national database for domestic violence prevention and victim protection**

After the government submitted the request, CNPD's Opinion 8/2024 addresses the new database regulation concerning domestic violence (Law No. 112/2009, 16 September and Law Proposal No. 28/XIV/1) highlighting the necessity of a thorough data protection impact assessment, particularly given the sensitive nature of the information involved.

Concerns related to the purposes and legal basis of the processing were raised. CNPD understood that the law seems to have wanted to extend the processing of data in the database to crimes other than domestic violence, which could violate the principles of proportionality and minimization of the processing of personal data, in terms of necessity and adequacy (art. 5(c) of the GDPR).

This opinion emphasizes concerns regarding the processing of personal data across multiple public entities. Additionally, the CNPD points to gaps in data security protocols, excessive data retention periods and the lack of a clear procedure for minimizing access to sensitive information. As a result, the CNPD recommended the development of robust measures to safeguard individuals' privacy within this new system, as well as provided the following indications:

- The legal basis for processing considered in the regulation needs to be reviewed;
- The criteria for the inclusion of personal data, aligning them with the standards set forth by the law, must be reassessed;
- The data retention periods shall be reviewed; and
- There should be given alternative authentication methods, besides the use of the national ID card and digital mobile key (CMD), should be provided.



## Legal opinion on necessary information elements for anti-money laundering/counter-terrorist financing compliance

Banco de Portugal, Portugal's national competent authority within European Banking Supervision, requested the CNPD to issue an opinion on a project aimed at defining the information elements that financial entities must report annually to the bank in the context of anti-money laundering (AML) and counter-terrorist financing (CTF).

On Opinion 01/2024, the CNPD concluded that the processing of data of the executive member of the management body appointed under the terms of Law No. 83/2017, the compliance officer, the person responsible for compliance with the regulatory framework for the prevention of money laundering and terrorist financing and their substitutes is appropriate and necessary for Banco de Portugal's supervisory functions, adhering to the principle of data minimization under Article 5(1)(c) of the GDPR.

## Legal opinion on the Cooperation Protocol on preventing and combating money laundering and terrorist financing

CNPD issued Opinion 13/2024 concerning the Protocol submitted by Banco de Portugal for collaboration with Serviço de Informações de Segurança (SIS), the Portuguese Secret Service and Intelligence Agency. This cooperation is aimed at combating money laundering and the financing of terrorism. A data protection impact assessment was requested by CNPD, which was duly submitted for review.

CNPD found that:

- More robust security measures should be adopted to ensure the protection of personal data involved in this interagency cooperation;
- The protocol must be revised to reflect the findings of the DPIA in order to ensure that it is aligned with the proper procedural safeguards; and
- One specific clause of the protocol must be further elaborated to ensure the implementation of techniques that guarantee the traceability of information flow and access controls, a vital step for maintaining transparency and accountability in handling sensitive data.

## CNPD's Activity Plan (2024-2026)

In 2023, CNPD approved a 2024 Activity Plan, which is part of a three-year activity plan for 2024-2026 that has already been published, focusing on specific goals:

- Reinforce the protection of citizens' personal data, including tools for disseminating the CNPD's mission and action;
- Ensure strategic observation of emerging risks and opportunities with technological innovation and security through deepening knowledge in the technological domain; and
- Reinforce and strengthen the regulation of personal data in Portugal, including collaboration between national and international entities. To achieve these objectives, the CNPD defines 20 operational actions, including the creation of databases, definition of campaigns, management and cooperation strategies and initiatives.

Moreover, in July 2024, CNPD approved its 2025 Activity Plan, adding three more activities to the list of 20 activities established in the 2024's plan, one of them being related to CNPD's regulation of data protection rights in the digital environment.

# ? What are the most relevant **cybersecurity updates**?

## CNCS report on cybersecurity in Portugal – risks and conflicts

The Cybersecurity Observatory of the Portuguese National Cybersecurity Center (CNCS) published its 2024 report, providing an in-depth analysis of the cyberthreats affecting Portugal's national cyberspace over the past year, presenting key data on cyberthreats affecting Portugal's national cyberspace.

This report is divided into two key sections:

- Incidents and cybercrime: Offers statistical data and insights on cyberthreats encountered in the previous year; and
- Threats and trends: Analyzes the underlying causes of incidents and forecasts future trends in cyber risks.

The report also provides general recommendations aimed at strengthening national cybersecurity efforts, including:

- Encouraging the creation of sectoral and regional cybersecurity communities for the sharing of threat and compromise indicators between organizations;
- Aligning the identification and update of the threat landscape with risk mitigation actions, especially through human and technological capacity-building programs; and
- Raising awareness among citizens and employees on cybersecurity best practices, particularly regarding threats that exploit human vulnerabilities.

Furthermore, the report includes specific recommendations tailored to each type of cyberthreat, ensuring a comprehensive approach to addressing both current and emerging risks in the national cyberspace.

## Guidelines for reporting cybersecurity incidents

The “*Referencial de Comunicação de Risco e de Crise em Cibersegurança*”, developed by CNCS, serves as a set of guidelines for national organizations to effectively manage cybersecurity risks and crises through communication.

This document is designed to support organizations in enhancing their internal risk management and crisis communication strategies, outlining essential steps, roles, and functions within communication teams, encouraging continuous improvement of their strategies.

Aligned with the National Cybersecurity Strategy, the guidelines are not prescriptive but provide a flexible framework for organizations to develop tailored policies and plans according to their specific contexts, incorporating international best practices from countries such as Belgium, Canada, Spain, the US, France, and the UK, along with adherence to the ISO 22361:2022 standard on crisis management.

The overarching goal of these guidelines is to establish a national reference for planning and managing communication related to risks and crises in the cybersecurity domain.



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

## **IRIS project**

The IRIS project, was developed by the Supreme Court of Justice in collaboration with INESC ID since 2020, and presented in the past year, introduces an innovative AI tool aimed at enhancing the management of court documents.

By utilizing optical character recognition (OCR) and anonymization techniques, this tool streamlines the handling of large data volumes while ensuring the protection of personal information. This project includes two key functionalities: a database of jurisprudential decisions that will promote transparency and improve access to court rulings, and an anonymization tool for judgments that will be made available to all courts through a protocol with the Superior Council of the Judiciary.

The initiative underscores the judiciary's commitment to responsibly adopting AI technologies, representing a significant step towards improving operational efficiency within the legal framework while safeguarding individual privacy.

## **Approval of the proposed EU AI regulation**

On 21 May 2024, the European Council approved the Regulation on Artificial Intelligence (AI Act). The EU AI regulation entered into force on 1 August 2024, being directly applicable to Portugal.

This regulation aims to establish harmonized rules on artificial intelligence, provides AI developers and deployers with clear requirements and obligations regarding specific uses of AI. At the same time, the regulation seeks to reduce the administrative and financial burden on businesses, especially small and medium-sized enterprises.

## **Digital Transformation Strategy for Public Administration**

The mid-term report of Portugal's Digital Transformation Strategy for Public Administration (ETDAP 2021-2026) highlights the adoption of transformative technologies such as the use of artificial intelligence to improve decision-making and public service delivery. Guidelines on this matter were launched to ensure responsible AI use, and a risk assessment tool is available for all AI projects in public administration.

Additionally, ongoing AI projects are being evaluated against ethical and accountability criteria to ensure they align with best practices for responsible innovation in the public sector.

## **CNPD's Activity Plan (2024-2026)**

In July 2024, CNPD approved its 2025 Activity Plan, as per referred above, adding three more activities to the list of 20 activities established in the 2024's plan, one of them being related to CNPD's goal of strengthening its activity in matters regarding the use of artificial intelligence.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## NIS2 to be transposed in the following months

As Portugal prepares to transpose the Network and Information System Directive 2022/0383 (NIS2), *Centro Nacional de Cibersegurança* (CNCS) remains responsible for overseeing the proper implementation, just as it did for the original NIS Directive.

NIS2 aims to enhance cybersecurity resilience across essential sectors, improve reporting requirements for significant incidents and extend obligations to medium and large-sized entities.

The CNCS will play a critical role in ensuring compliance with these new measures, which target stronger security protocols and improved risk management strategies across the supply chain and critical infrastructures.

## National AI strategy

Portugal's National AI Strategy 2030 outlines key areas where AI is expected to grow and be regulated, focusing on both development and ethical concerns. Key concerns include ensuring AI aligns with GDPR to safeguard data protection and privacy, while promoting algorithmic transparency to prevent bias and uphold fairness.

The strategy promotes AI development in public administration to enhance efficiency while protecting individual rights, highlighting critical areas for expansion including fostering AI literacy, advancing sustainable AI solutions, and aligning research and development with European AI policies.

## Enforcement of the EU AI Act

The enforcement of the majority of the EU AI Act's provisions will commence on 2 August 2026, even though there will be provisions that will be effective by 2 February 2025 (Chapter I and II), 2 August 2025 (Chapter III Sec. 4, Chapter V, Chapter VII, Chapter XII and Article 78, with the exception of Article 101) and 2 August 2027 (Article 6(1)). In the meantime, providers of high-risk AI systems are encouraged to comply with these provisions so that the transition is less abrupt.

It is expected that guidelines and laws will be produced to ensure that the EU AI Act is implemented in the national legal order.

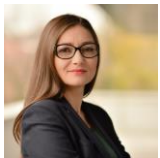
## New guidelines on artificial intelligence

The CNPD is expected to issue new guidelines on the use of artificial intelligence soon, providing an updated framework on AI applications in compliance with data protection laws, building upon existing regulations to address current challenges and risks, specially considering that CNPD established new goals and activities related to artificial intelligence to its 2025 Activity Plan, moving one step further towards AI regulation.

This initiative aims to ensure transparency, fairness, and the safeguarding of personal data in AI systems, reflecting the CNPD's commitment to adapting to technological advancements while upholding the principles of the GDPR.

# Romania

## Contacts



**Georgiana Singurel**

Partner, Deloitte Legal Romania  
[gsingurel@reff-associates.ro](mailto:gsingurel@reff-associates.ro)



**Silvia Axinescu**

Senior Managing Associate, Deloitte Legal Romania  
[maxinescu@reff-associates.ro](mailto:maxinescu@reff-associates.ro)

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

## **Data processing activities carried out by public institutions and bodies**

### **Increased oversight and involvement by ANSPDCP**

During 2024, the National Authority for the protection of personal data (ANSPDCP) has increased its interest in data processing activities carried out by public institutions and bodies. The following actions merit mentioning:

- Clarification of the framework applicable for sanctioning public institutions. According to the Romanian law implementing the GDPR (i.e., Law 190/2018) ANSPDCP may apply tiered sanctions to public institutions and bodies, namely (i) a warning is issued and a remedial plan for conformation is proposed; and (ii) if the public body does not comply with the measures in the remedial plan, ANSPDCP has the authority to also apply fines, ranging from RON 10,000 to 200,000. (Source: [Comunicat Presa 23.07.2024 \(dataprotection.ro\)](#))
- Investigation into the methods of personal data collection as part of a financial aid program implemented by the Bucharest First District Hall, which resulted in the imposition of a tiered penalty framework. (Source: [Comunicat Presa 31 01 2024 \(dataprotection.ro\)](#) and [Comunicat Presa 06 03 2024 \(dataprotection.ro\)](#))
- Training sessions organized for the benefit of the personnel of the Ministry of Home Affairs, which is the government structure responsible for organizing the Romanian Police Force (including Border Police), Romanian Inspectorate for Immigration, and Romanian Inspectorate for Emergency Situations, etc. (Source: [Comunicat Presa 18 04 2024 \(dataprotection.ro\)](#))

## **Use of audio recordings as part of legal proceedings**

### **Evidence admissibility**

The High Court of Cassation and Justice (ICCJ) was called to interpret the legal provisions to answer the question whether audio recordings of phone conversations between employees or between employees and other representatives of the employer are admissible as evidence (in labor law litigation and when requested by the employee) when the participants to such conversations were not informed that the recording takes place, nor had consented to being recorded.

The ICCJ ruled that such evidence is in principle admissible, subject to ensuring a fair balance between the right to evidence, on the one hand, and the right to private life, on the other hand, meaning that the admissibility of evidence must be indispensable to the exercise of the right to evidence and strictly proportional to this purpose.

(Source: [Minuta deciziei nr. 39 din 16 septembrie 2024 – Înalta Curte de Casație și Justiție a României \(iccj.ro\)](#))



## Cooperation of ANSPDCP with Polish Supervisory Authority

### Fine of €17,000 applied to Romanian Branch of Polish Bank

A Romanian customer of Alior Bank SA Warsaw Bucharest Branch, lodged a complaint with ANSPDCP claiming that the controller had sent unsolicited messages both by email and SMS to the data subject, although the data subject had previously requested the deletion of their data and that the contractual relationship with the controller was terminated and, consequently, the related bank accounts of the data subjects were closed.

The ANSPDCP launched an investigation during which it consulted with the Polish DPA considering that the IT system of the controller's branch in Romania was integrated into the centralized system of Alior Bank SA Warsaw, based in Poland. Consequently, the messages communicated to customers after the date of termination of the contractual relationship with the financial institution were sent by the technical department of Alior Bank SA Warsaw in Poland.

Following the internal enquiries at the level of the Romanian branch, it became clear that when a contractual relationship with customers ended, the controller continued to monitor their activity and send messages on certain operations.

ANSPDCP sanctioned the Romanian branch with a fine of €17,000 and imposed the following corrective measures.

- To regularly monitor compliance with the principles and rules set out in Article 5 GDPR and Article 6 GDPR to avoid unlawful processing of personal data of data subjects and, in case necessary, to reconfigure systems or applications used in the processing of personal data; and

- To inform its Polish branch about the above-mentioned to properly implement the data protection principles under GDPR.

(Source: [Comunicat Presa 12.01.2024 \(dataprotection.ro\)](#))

## Comminatory fine applied to public institution

### Bucharest First District Hall fined RON 159,000

ANSPDCP launched an investigation into personal data collection method used by the First District Hall to run a financial aid program.

The public institution refused to cooperate during the investigation as it did not provide the information requested by ANSPDCP.

This resulted in the tiered application of the following sanctions: (i) a warning was issued and the District Hall was ordered to provide the information; (ii) as the institution did not comply with the order within the specified time frame, a fine of RON 10,000 was applied together with the corrective measure of obliging the District Hall to supply the information; and (iii) since the District Hall failed to comply in the additional time frame granted by ANSPDCP, the controller was fined with a comminatory fine of RON 159,000 – such amount being calculated as the equivalent of 53 days of non-compliance at a daily rate of RON 3,000.



# ? What are the most relevant **cybersecurity updates?**

## **ANSPDCP role in security breaches**

### **ANSPDCP maintains an active role in sanctioning cases where security of personal data is affected**

Throughout 2024 we noticed an increase in the number of fines applied by ANSPDCP in cases of breaches of security. Some examples include:

- Fine of €3,000 for IT company for an unauthorized disclosure of personal data on the internet (via its website). ANSPDCP ordered that the controller implements (i) a process of periodic testing, evaluation and assessment of all systems and their subsequent changes, and (ii) password complexity procedures, especially for administrator accounts, which include specific requirements regarding: the minimum length of the password, the variety of characters, its expiration period, as well as the impossibility of reusing a previously registered password. (Source: [Comunicat Presa 15.01.2024 \(dataprotection.ro\)](#))
- Fine of €5,000 applied to self-storage facility company who was the target of a cyberattack which resulted in the breach of availability and confidentiality of personal data. ANSPDCP also ordered that the controller implements access monitoring/logging systems which include a retention period of access logs of at least 30 days, including the introduction of a back-up process. (Source: [Comunicat Presa 05\\_03\\_2024 \(dataprotection.ro\)](#))
- Fine of €1,000 applied to an NGO who was the target of a cyberattack which resulted in the loss of personal data on the NGO's server. ANSPDCP also ordered the controller to review the technical and organizational measures applied to secure the data, especially those which prevent third parties accessing their servers from outside of the network. (Source: [Comunicat Presa 10.09.2024 \(dataprotection.ro\)](#))

## **Guidelines for the general public**

### **DNSC issues guidelines targeted at educating the general public**

During 2024 DNSC issued a number of guidelines to educate the general public towards cyber resilience. The guidelines are:

- Guidelines for protecting and recovering social media accounts;
- Guidelines for responding to cybersecurity incidents;
- Best practices for remote-accessing applications;
- Analysis of Ov3r Stealer malware and its impact cybersecurity;
- Guidelines for protection of personal data and cybersecurity for children, parents and teachers;
- Guidelines for data protection during holidays; and
- Guidelines regarding the strategic principles for cybersecurity in company management.



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

## Guidelines on deepfakes

### **DNSC issues two guidelines regarding deepfakes**

DNSC issued two guidelines on the topic of deepfakes:

#### **1. Guideline targeted at the general public**

The first guideline is targeted at the general public (i.e., anyone aged over 18) and its purpose is to raise awareness and facilitate understanding of the use Generative AI tools to create video, audio or image content, and to aid in the detection of the use of such tools. The guideline explains what a deepfake is, what technology underpins it and gives some examples of such manipulated content. Additionally, the guideline also emphasizes the risks posed by the deepfake and presents some practical ways to recognize deepfakes alongside with actionable steps, such as reporting the content.

#### **2. Guideline targeted at companies**

The second guideline, which is targeted at companies, highlights the risks and impact that deepfakes can have on the business processes. Similarly to the first guideline, it provides actionable steps and recommendations for the detection of deepfakes and minimizing their impact.

## National strategy for AI

### **The government formally approves the national strategy for AI**

Government Decision No. 832/2024 (GO) regarding the approval of the National Strategy for AI came into force on 25 July 2024.

The document recognizes specific tasks of various public institutions, including ministries, in the development and deployment of AI, as well as for purposes of education in the field of AI. Ministry of Research, Innovation and Digitalization and the Authority for the Digitization of Romania are the main public bodies charged with overseeing the implementation of the strategy. Such institutions are also subject to reporting obligations, thus highlighting the accountability regime imposed on them.



## What are the most relevant expected developments in data protection, cybersecurity and AI?

### **Draft law on responsible use of technology in the context of deepfakes**

#### **Updates of the legislative process**

The legislative process for a draft law on the responsible use of technology in the context of started and was approved by the senate in 2023. In 2024, the legislative process progressed, with the draft law now pending approval by the second chamber (Chamber of Deputies) which is the decision forum in this legislative procedure. It is expected that the draft law shall come into force during 2025.

### **Entry into force of new legislation**

#### **NIS2 implementation law**

A legislative proposal for the transposition of the NIS2 Directive into national law has already been drafted, and it is anticipated that the draft emergency ordinance will be adopted by the end of 2024.

#### **DORA guidelines**

2024 has seen the NBR organize voluntary compliance and dry run exercises in which it involved major banks from Romania. It is expected that the results of these actions shall take the form of guidelines or best practices for DORA implementation.

# Senegal

## Contacts



**Badara Niang**

Managing Partner, Deloitte Senegal

[bniang@deloitte.fr](mailto:bniang@deloitte.fr)



**Eva N'Konou**

Quality and Risk Director, Deloitte Senegal

[enkonou@deloitte.sn](mailto:enkonou@deloitte.sn)



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

## **General deliberation No. 00645/CDP of 13 April 2023 on the use of biometric devices in the workplace**

In view of the proliferation of biometric devices used to control access and manage employees' time in the workplace, on 13 April 2023 the Commission for the Protection of Personal Data (CDP) adopted a general resolution laying down rules for the use of biometric devices in the workplace.

As a rule, one of the major clarifications provided by this deliberation is that the collection and processing of biometric data derived from facial recognition, the iris of the eye and voice recognition are not authorized by the CDP, except in the case of biometric devices installed in strategic or sensitive public establishments.

Furthermore, it is specified that visitors and advisers who visit workplaces on an occasional basis are not affected by the collection and processing of personal data by biometric devices.

As with the installation of video surveillance systems, the installation of a system for collecting and processing biometric data in the workplace requires prior notification of the persons concerned by means of a memo, information note or any other duly notified document.

## **Launch of the national data strategy**

Senegal has decided to adopt a national data strategy based on four fundamental principles: protection of privacy, transparency, fairness, and security.

This strategy, validated on 25 July 2023, will shortly be submitted to the council of ministers for approval. It takes into account the regulatory framework, data collection infrastructures, e.g., data centers, and the storage and use of data.

Through this initiative, Senegal aims to position itself as the largest regional digital platform via the Senegal Digital Strategy (SN 2025).

# ? What are the most relevant **cybersecurity updates**?

## **Completion of 18 out of 97 reforms, according to the updated SN2025**

Developed in 2016 as part of the implementation of the Emerging Senegal Plan (PSE), the “Digital Senegal 2025” (SN2025) strategy is designed to serve as a catalyst for the modernization of the economy and the improvement of competitiveness.

Updated in October 2019 by the Senegalese authorities, 18 reforms have been carried out to date, the main ones being:

- The development of a national broadband and a very high-speed broadband plan;
- The revision of the method of pricing radio-relay links in view of the development of data traffic related to very high-speed mobile broadband;
- Removing barriers to entry for new players in the Internet access segment (ISP/ISP);
- The implementation of the regulatory framework allowing the allocation of authorizations to infrastructure operators (submarine cables, fiber optics, Senelec, etc.);
- The development of a national policy document on cybersecurity and the fight against cybercrime;
- The development of the sectoral telecommunications policy letter; and
- Updating the Telecommunications Code and texts on the information society.



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

## **Launch of the process to formulate Senegal's national AI strategy**

The process was launched by Senegal's Minister of Communication, Telecommunications and the Digital Economy on 17 May 2023 during "Senegal Connect" Digital Week and took four months to complete.

The inclusive and participatory approach focused on:

- One international benchmarking (between May and July 2023);
- Participation in the UNESCO workshop on assessing Senegal's level of maturity and the ethics of AI (August 2023);
- Three collaborative consultation and co-construction workshops with the public, private and associate ecosystem (June and July 2023);
- Bilateral interviews with key players (July 2023); and
- One awareness-raising workshop on the challenges of AI and alignment with the data strategy organized by GiZ in partnership with the AU-EU D4D Hub (July 2023).



## What are the most relevant expected developments in data protection, cybersecurity and AI?

### Reform of the draft law on the protection of personal data

The Commission for the Protection of Personal Data (CDP) of Senegal recently organized a workshop with the aim of updating the texts relating to personal data. This gathering was held on 10-11 October 2024 and aimed to modernize the bills to align them with the country's new digital sovereignty strategies, in accordance with the directives of the head of state.

Indeed, this workshop aimed to modernize Senegalese laws on personal data by adapting them to digital realities. It brought together the Ministry of Communication and Digital Economy, the private sector and civil society to discuss stricter protection standards and the country's digital sovereignty.

Since 2017, the CDP has been working with various sectors to create legislation that takes into account technological advances and security concerns. The objective is to effectively protect citizens' data.

Strengthening this legislation will allow Senegal to improve its digital security, support its economic development and become a leader in data protection in West Africa. It will also strengthen citizens' and businesses' trust in digital platforms.

### Acceleration of the digitalization of administrations

On the occasion of the council of ministers held on 12 June 2024, the president of the Republic invited the prime minister and the minister in charge of telecommunications and digital affairs to accelerate the full digitalization of administrations and the definition of an advanced national cybersecurity strategy in order to strengthen trust in the digital sector.



## Implementation of a roadmap for Senegal's national AI strategy

The Ministry of Communication, Telecommunications and Digital Economy (MCTEN) has initiated a process of formulating a national strategy on AI taking into account Senegal's specific challenges while ensuring its alignment with the Digital Senegal 2025 digital strategy and the Emerging Senegal Plan (PSE).

To this end, three waves of actions, including 52 actions, will be implemented in 2024-2025. The priority actions are as follows:

- Action 1.1: Develop in collaboration with the AI ecosystem an international training framework for data science and AI, assess the gap with existing training and the skills of trainers and establish a ramp-up plan and a mapping, to be promoted through a common label.
- Action 1.6: Develop, in collaboration with the AI ecosystem, an AI monitoring and business intelligence observatory (skills needs in the sector, necessary training, research programmes and collaborative projects, etc.) to feed the future AI cluster, update the training repository and feed the strategy.
- Action 1.7: Implement, in collaboration with the AI ecosystem, a cycle of seminars to raise awareness among key stakeholders in Senegal on the opportunities and risks of AI and its ethical and environmental challenges, with a focus on the multidisciplinary nature of the participants.
- Action 2.5: Create an AI campus, a space for gathering, expression and action for AI communities and startups and support their animation programs.
- Action 2.6: Access to AI infrastructures: integrate an application layer of AI services into public data centers, make access to these data centers and the supercomputer simple and affordable.
- Action 2.10: Implement a special Startup Act program dedicated to data science and AI.
- Action 4.1: Set up a regional program of partnerships/collaborations on AI with the AI countries and communities of the West Africa and North Africa region, in collaboration with the AI campus (bilateral country meetings but also with UEMOA, ECOWAS).
- Action 4.2: Implement this partnership programme at EU level to make it possible to form partnerships giving access to greater resources (France, Germany, Belgium, Luxembourg, etc.).
- Action 6.1: Development and launch of a major national consultation on the challenges of AI, the orientations proposed by the national strategy in terms of governance and the expectations of stakeholders (this action could be driven either by the prefiguration structure of the AI regulatory body, or by the prefiguration structure of the AI cluster, both to install).
- Action 6.5: Implement a transversal management of the AI strategy with the required technical expertise and an information system.

# Serbia

## Contacts



**Stefan Antonić**

Director, Deloitte Legal Serbia  
[santonice@deloittece.com](mailto:santonice@deloittece.com)



**Igor Denčić**

Managing Associate, Deloitte Legal Serbia  
[idenic@deloittece.com](mailto:idenic@deloittece.com)

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

## Activities of the Commissioner for Personal Data Protection in 2023

- **Extensive activities:** During 2023, 5,211 cases were formed and 4,930 were completed, including 731 inspections (549 regular and 182 extraordinary).
- **Corrective measures:** 51 corrective measures, including warnings, were adopted, with 721 field inspections and 33 written inspections. The largest number of inspections was related to educational institutions (75.3%).
- **Complaints and misdemeanors:** The commissioner filed 10 requests for misdemeanor proceedings and issued five misdemeanor orders. It dealt with 393 petitions, and 36 were forwarded to other bodies.
- **Education:** Checklists have been developed to help authorities comply with regulations. By the end of the year, 4,295 of the 5,356 controllers had responded to the checklists.
- **Records and representatives:** 1,401 data protection persons were registered, and 47 decisions on the appointment of foreign representatives were received.

In 2023, the commissioner continued the practice of opening offices outside the headquarters in Belgrade. Following the office opened in Novi Sad at the end of 2022, an office was opened in Niš. By the end of 2024, the opening of a third office outside Belgrade is planned, specifically in Kragujevac.

The commissioner highlights the shortcomings of the Law on Protection of Personal Data as the main obstacles to the realization of the right to personal data protection. Although this law offers better protection, many provisions are unclear, and there are issues with the implementation of mechanisms that are not part of the domestic legal system. Additionally, insufficiently developed procedural provisions regarding complaints to the commissioner lead to legal uncertainty due to the possibility of overlapping procedures.

## Strengthening data protection: collaborative efforts in the region

In light of the new privacy policy of Meta, effective 26 June 2024, for users in Serbia, the commissioner warns that users have not been informed about this policy, which involves the processing of their data for the purpose of developing artificial intelligence. Additionally, X Corp. and Twitter International Unlimited Company are engaging in unauthorized data processing for similar purposes without prior notice.

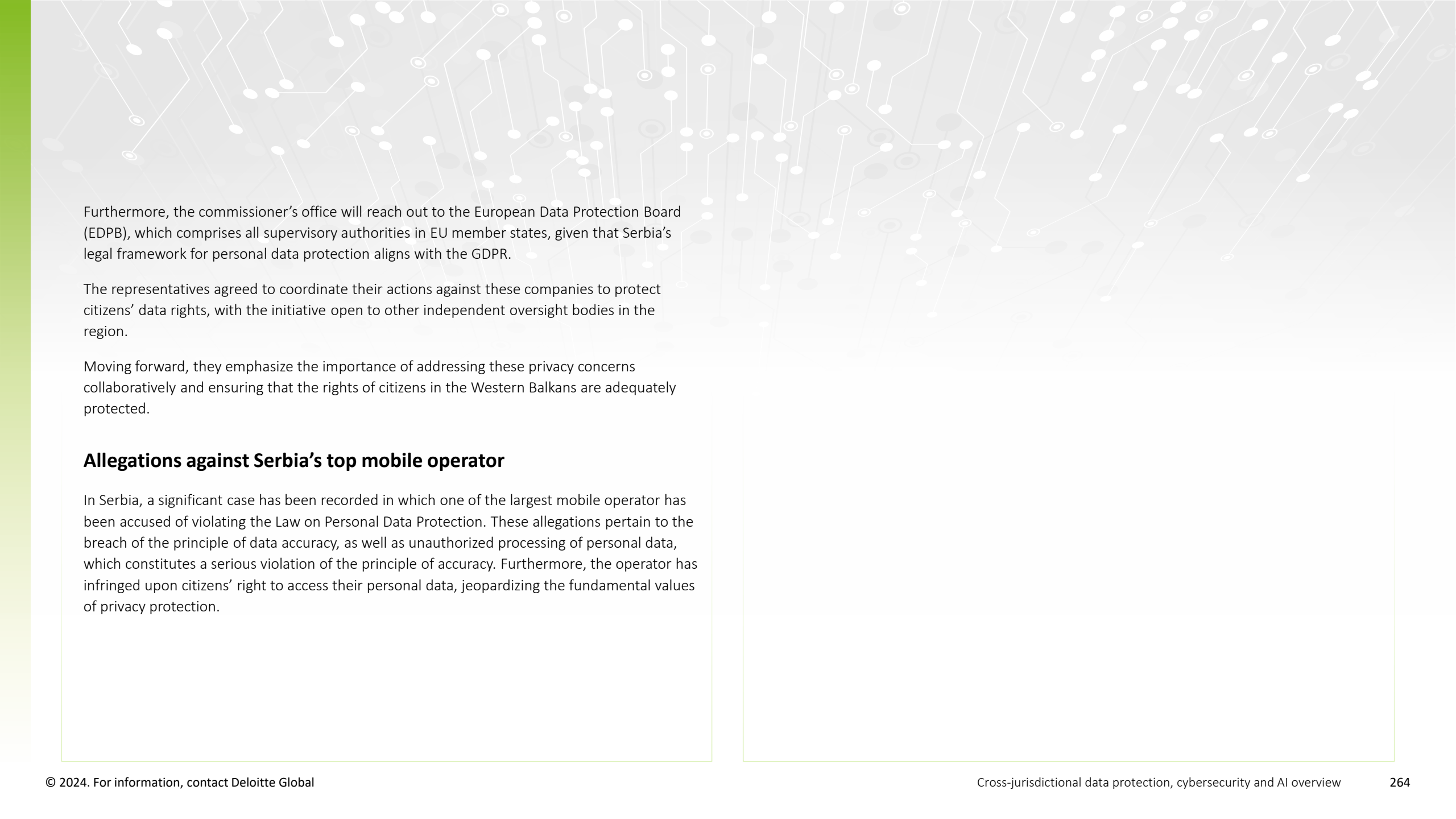
The commissioner alongside representatives from independent data protection authorities from the Western Balkans, met in Sarajevo on 4 September 2024.

Key points discussed include:

- Both companies initiated processing personal data without informing users in non-EU Western Balkan countries; and
- Neither company has designated a representative for data processing in Serbia, Montenegro, and Bosnia and Herzegovina.

To address these issues, the commissioner is taking steps to establish contact with these companies in the United States, reminding them of their obligation to designate representatives in accordance with the law. This is vital for ensuring equal treatment of Serbian citizens and EU citizens, especially considering that the use of personal data of EU citizens by Meta has been postponed.

Efforts are also being made to contact the Data Protection Commission of Ireland, the authority responsible for Meta Platforms Ireland Inc. and Twitter International Unlimited Company as data controllers.



Furthermore, the commissioner's office will reach out to the European Data Protection Board (EDPB), which comprises all supervisory authorities in EU member states, given that Serbia's legal framework for personal data protection aligns with the GDPR.

The representatives agreed to coordinate their actions against these companies to protect citizens' data rights, with the initiative open to other independent oversight bodies in the region.

Moving forward, they emphasize the importance of addressing these privacy concerns collaboratively and ensuring that the rights of citizens in the Western Balkans are adequately protected.

### **Allegations against Serbia's top mobile operator**

In Serbia, a significant case has been recorded in which one of the largest mobile operator has been accused of violating the Law on Personal Data Protection. These allegations pertain to the breach of the principle of data accuracy, as well as unauthorized processing of personal data, which constitutes a serious violation of the principle of accuracy. Furthermore, the operator has infringed upon citizens' right to access their personal data, jeopardizing the fundamental values of privacy protection.



# ? What are the most relevant **cybersecurity updates**?

## Law for the implementation of the NIS2 Directive

### Draft of the Law on Cybersecurity – post public debate

Summary of key points:

- **Purpose and scope:** The draft law sets out measures for protecting ICT systems from security risks, outlining the responsibilities of entities managing these systems. It establishes processes to achieve a high level of information security and defines the roles of various governmental bodies in enforcing these protections.
- **Principles of information security:** The draft law emphasizes principles like risk management, comprehensive protection across all levels, and ensuring all stakeholders are aware and skilled in maintaining information security.
- **Critical ICT systems:** It categorizes ICT systems into essential and important entities, based on their societal and economic impact, and outlines obligations for operators of these systems (e.g., in sectors like energy, transport, healthcare, and banking).
- **Obligations of ICT system operators:** Operators must implement appropriate technical and organizational measures, conduct regular risk assessments, and submit reports on security incidents.
- **Incident reporting and management:** The draft law mandates that operators report incidents impacting system security to the relevant authorities within 24 hours. The draft law also sets up processes for responding to high-level incidents and national crises in information security.
- **Penalties:** The document outlines fines ranging from approx. €400 to €17,000 for failing to comply with the requirements set out by the law.

## Reasoning behind the adoption of a new Law on Information Security

As Serbia is in the process of accession to the EU, it assumed the obligation to harmonize its legislation, including [the adoption of a new Law on Information Security](#).

Key points include:

- **Legal basis:** The law is grounded in the Serbian constitution and aims to support the country's economic and technological growth; and
- **EU alignment:** The law seeks to harmonize with EU directives, including the EU Cybersecurity Act and NIS2 Directive, aiming to strengthen Serbia's cybersecurity framework, especially for ICT systems critical to national functions.

Key provisions:

- Defines ICT systems of special importance and divides them into “priority” and “important” based on their significance to national security and economy;
- Introduces mandatory risk assessments for these systems and the development of incident response procedures; and
- Enhances the role of the National CERT (Computer Emergency Response Team) and establishes a Cybersecurity Office by 2027 to oversee incident management and coordination.

Objectives:

- Ensure safer use of ICT systems;
- Foster competition and digital services in the market;
- Facilitate foreign and domestic investments in cybersecurity; and
- Create conditions for the safe data handling and electronic services.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Personal Data Protection Strategy for the period of 2023-2030

This strategy guarantees that there will be an improvement of the data protection mechanism in the form of increasing the capacity of the commissioner and other controllers and processors, by introducing training programs at higher education institutions, establishing appropriate records, obligations to pass internal acts, etc.

The strategy acknowledges the importance of increasing actions by public prosecutors in response to criminal complaints from the commissioner and citizens, along with a greater percentage of cases being successfully resolved in court to uphold rights related to personal data protection. Additionally, it highlights the necessity of establishing more regional offices for the commissioner and increasing the number of specialized data protection officers.

The strategy announced that the penal policy for breach of obligations in personal data protection would be much more severe, and that the amount of fine would depend on the company's income.

## Decision on the establishment of a Council for Artificial Intelligence

The Serbian government has decided to [establish a Council for Artificial Intelligence](#), whose task will be to align and coordinate activities related to implementing the strategic framework for developing artificial intelligence, as announced in the Official Gazette.

Tasks will also include monitoring the implementation of planned measures and activities, observing the state, needs, and standards of AI development and application in Serbia and globally. The council will have an advisory role, preparing proposals, recommendations, and standards, providing opinions, and expert explanations on all issues related to the development and application of AI in Serbia. The council will be established for five years from the date this decision takes effect.

## New strategy for the development of AI for 2024-2030

### The strategy has gone through public discussion and is waiting to be adopted

Serbia develops and applies AI and uses it for economic and scientific development and for the benefit of its citizens. The overall objective of [the strategy](#) is to accelerate the development of national resources for the development of artificial intelligence in the economy and education, ensuring the availability of artificial intelligence for all citizens.

The specific objectives of the strategy are:

- Improving education and promoting artificial intelligence;
- Creation and harmonization of legal framework and institutions for the safe, secure and responsible application of artificial intelligence;
- Promoting and facilitating the development of artificial intelligence and AI-based solutions;
- Increasing the use of artificial intelligence in all segments of society and the economy;
- Data is the most important resource for the development of artificial intelligence; and
- Improving the infrastructure and resources necessary for the development of artificial intelligence.

## First meeting of the working group for drafting the Serbian Artificial Intelligence Law (3 June 2024)

The Ministry of Science, Technological Development, and Innovation with strong support from the Institute for Artificial Intelligence is [planning to present the draft of the Artificial Intelligence Law by 31 March 2025](#).

# Singapore

## Contacts



**Joanna Yap**

Managing Director, Sabara Law LLC (member of the Deloitte Legal network)

[joayap@sabaralaw.com.sg](mailto:joayap@sabaralaw.com.sg)



**Gretchen Su**

Director, Sabara Law LLC (member of the Deloitte Legal network)

[gretchensu@sabaralaw.com.sg](mailto:gretchensu@sabaralaw.com.sg)



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

## Children's personal data in the digital environment

In March 2024, the Personal Data Protection Commission (PDPC) released [advisory guidelines on the Personal Data Protection Act 2012 \(PDPA\) for children's personal data in the digital environment](#). The guidelines target organizations offering online products or services which are likely accessible by children. Organizations are now encouraged to adopt the following guidelines when handling children's personal data, children's consent management and the various data protection practices suggested in this guide.

The suggestions found in the guideline include, but are not limited to:

- Organizations must use language, when drafting terms and conditions, that is readily understood by children so that they can comprehend the consequences of them giving consent.
- Organizations must ensure children are able to easily withdraw consent for providing personal data.
- Organizations should adopt data minimization policies to limit collection of children's personal data. This can be done by disabling the geolocation function by default.
- Organizations handling children's personal data should implement the basic and enhanced practices as listed in the PDPC's Guide to Data Protection Practices for ICT systems, to address risks and harms that could potentially affect children.
- Organizations should inform individuals when there is a data breach, and if the child is unable to understand the consequences of such data breaches, the organization should reach out to the child's parents or guardian.
- Organizations should conduct a Data Protection Impact Assessment before releasing online products or services that can be accessed by children, to identify and address personal data protection risks.

## The use of personal data in AI recommendation and decision systems

In March 2024, the PDPC released [advisory guidelines on the use of personal data in AI recommendation and decision systems](#). The purpose of this guideline is to provide organizations with clarity and certainty on how and when they can use personal data to develop and deploy machine learning models. Additionally, these guidelines seek to assure consumers that their personal data is handled in accordance with the PDPA by implementing guidance and best practices for organizations.

The suggestions in this guideline include, but are not limited to:

- Organizations, when obtaining consent to utilize personal data to train their AI system, if they are AI developers, can consider relying on the business improvement or research exceptions. This enables organizations to bypass the need to get consent, provided that the personal data is used for purposes as listed in the guidelines.
- For the business improvement exception, the purposes can range from learning or understanding behavior of individuals to improving and enhancing existing goods and services or developing new goods or services.
- For the research purpose exception, the purposes can be to conduct broader research and development.
- Organizations are encouraged to anonymize datasets of personal data, limit volume of personal data used to train the AI system, and adhere to PDPA obligations such as consent, notification and accountability,
- Organizations should be transparent in their usage of personal data to the AI system.
- Organizations can use the AI Verify tool (see further discussion) to validate the performance of their AI systems.



## Privacy Enhancing Technologies Sandbox

[Privacy Enhancing Technologies \(PETs\) Sandbox](#) enable businesses to gain insight from data whilst ensuring that the standards of personal data protection, data privacy and the safeguard of commercially sensitive information are upheld.

Specifically, by removing or protecting personally identifiable information, PETs can help businesses optimize the use of data without compromising personal data. PETs address many of the limitations in working with sensitive, personal data and opens new possibilities by making data access, sharing and collective analysis more secure.

In July 2023, the Infocomm Media Development Authority (IMDA) partnered with Google to launch the IMDA-Google: PET x Privacy Sandbox, which allows various companies to collaborate with PET digital solution providers to develop use cases and pilot PETs.

To encourage more use cases for GenAI, IMDA has also expanded the Sandbox to support Generative AI use cases, by exploring how PETs can unlock more data for Generative AI use cases whilst also addressing data protection risks.

Some case studies include:

- Grab: Transformed manual data tagging and clearance process to one that is autonomized by a language learning machine-based metadata tagging and automatic anonymization of data.
- Mastercard: Developed a proof of concept in IMDA's PET Sandbox program to investigate a product which is based on fully homomorphic encryption, serviced by a third-party supplier, for sharing financial crime intelligence across international borders.

## Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses

In February 2024, the [Joint Guide to ASEAN Model Contractual Clauses and EU Standard Clauses](#) was updated with the release of the implementation guide.

This is the second guide within the joint guide; which consists of the reference guide, first released in May 2023, and the newly-released implementation guide.

The purpose of the joint guide is to assist companies that operate across the Association of Southeast Asian Nations (ASEAN) and EU regions to understand the similarities and differences between the ASEAN model contractual clauses (MCCs) and the EU standard clauses (SCCs), and to operationalize the safeguards required under both sets of contractual clauses.

The joint guide highlights the obligations for controller-to-controller transfers and obligations for controller-to-processor transfers. Such obligations relate to data accuracy, security measures and limitation of purpose.

The joint guide also discusses:

- Data subject rights;
- Security and confidentiality;
- Third-party beneficiary rights and redress; and
- Onward transfer.

The joint guide offers companies non-exhaustive examples of best practices that they can consider implementing on a voluntary basis in their contractual arrangements for the allowance of cross-border personal data transfers.

## Proposed Guide to Synthetic Data Generation

In July 2024, the PDPC issued the [Proposed Guide to Synthetic Data \(SD\) Generation](#), to provide a comprehensive framework for businesses using SD generation as a Privacy Enhancing Technology (PET).

SD generation is gaining traction as it creates realistic data for AI model training without using actual sensitive data.

The proposed guide aims to help businesses make sense of SD, by explaining what SD is, how it can be used and the best practices in creating SD. It is intended for CIOs, CTOs, CDOs, data scientists, data protection practitioners, and technical decision-makers involved in generating and using synthetic data. The guide outlines best practices, governance controls, and risk assessments to mitigate re-identification risks associated with synthetic data.

A potentially significant use case is to drive the growth of machine learning by enabling AI model training, while protecting the underlying personal data. SD also addresses challenges related to data quantity and quality (e.g., insufficient or biased data) for AI model training which requires huge volumes of data by augmenting training datasets.

Another situation where synthetic data can be beneficial is data sharing. The proposed guide offers guidance for organizations on evaluating and handling privacy risks and includes technical, contractual, and governance strategies to safeguard data integrity.

Moreover, the proposed guide presents a comprehensive five-step process for creating synthetic data, emphasizing the need to balance data utility and privacy protection, and features case studies and practical examples to demonstrate effective practices in synthetic data generation.

The five-step approach to SD generation is:

- Know your data;
- Prepare your data;
- Generate synthetic data;
- Assess re-identification risks; and
- Manage residual risks.

The proposed guide provides examples of methods of SD generation using statistical methods and deep generative models and includes a checklist of good practices to adopt when generating SD to guard against any possible risk of re-identification.

This proposed guide will be offered as a resource within the IMDA PET Sandbox to assist businesses to understand SD generation techniques and potential use cases, particularly for AI.

# ? What are the most relevant **cybersecurity updates?**

## Cybersecurity (Amendment) Act 2024

In May 2024, the [Cybersecurity \(Amendment\) Act 2024](#) was passed to update the Cybersecurity Act 2018, which establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore, to keep pace with evolving technological operating contexts and the developments in the cyberthreat landscape.

Under the amended Cybersecurity Act, critical information infrastructure (CII) operators in Singapore will need to declare any cybersecurity outage and attack faced by their premises or along their supply chain, as long as it affects their services.

The Cyber Security Agency of Singapore (CSA) is also empowered to have oversight over the cybersecurity of Systems of Temporary Cybersecurity Concern (STCCs), which are computer systems that are critical to Singapore and are at a high risk of cyberattacks because of certain events or situations.

In addition, two new classes of regulated entities are designated as Entities of Special Cybersecurity Interest (ESCI) and Foundational Digital Infrastructure (FDI), which will be subject to a light-touch regulatory treatment. They will be required to adhere to cybersecurity codes and standards of practice, as well as reporting prescribed cybersecurity incidents to CSA, which will not be at the level of a CII.

- ESCI are entities which hold sensitive information or perform a function of national interest, such that their disruption could cause potential adverse effects on the defense, foreign relations, economy, public health, public safety, or public order of Singapore.

- FDIs are companies that provide digital infrastructure services that are foundational to our economy or way of life (such as cloud service providers and data centers) to shoulder responsibility for the cybersecurity of such digital infrastructure.

## Guidelines and Companion Guide on Securing AI Systems

In October 2024, the Cyber Security Agency of Singapore (CSA) issued the [Guidelines and Companion Guide on Securing AI Systems](#).

The guidelines are meant to provide evergreen principles to raise awareness of adversarial attacks and other threats that could compromise AI behavior and system security, and guide system owners on implementation of security controls and best practices to protect AI systems against potential risks, including existing cybersecurity risks such as supply chain attacks, and novel risks such as adversarial machine learning.

To help system owners manage security risks from the outset, CSA is working with AI and cybersecurity practitioners to develop a Companion Guide for Securing AI Systems. This is designed as a community-driven resource to complement the Guidelines for Securing AI Systems and is not mandatory or prescriptive. It curates practical measures and controls, drawing from industry and academia, as well as advice from resources such as the MITRE ATLAS database and OWASP Top 10 for Machine Learning and Generative AI.

The guidelines recommend that AI should be secure by design and secure by default, as with all digital systems. This proactive approach will allow system owners to secure AI throughout all five stages of its lifecycle:



- Planning and design: Raise awareness of AI security threats and develop risk assessments;
- Development: Supply chain security and protection of AI assets;
- Deployment: Secure infrastructure, establish incident management processes and AI benchmarking and red-teaming;
- Operations and maintenance: Monitor for security anomalies and establish vulnerability disclosure processes; and
- End of life: Ensure secure and proper disposal of data and model artefacts.





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

## Generative AI Evaluation Sandbox

In October 2023, the Infocomm Media Development Authority (IMDA) and the AI Verify Foundation launched the first-of-its-kind [Generative AI \(GenAI\) Evaluation Sandbox](#). The sandbox will bring global ecosystem players together through concrete use cases, to enable the evaluation of trusted AI products.

The AI Verify Foundation was set up by the IMDA in June 2023 to allow for collaborations and contributions from the global open-source community to develop AI Verify testing tools. In consultation with companies such as DBS, Meta, Google and Singapore Airlines, the foundation launched AI Verify, an AI governance testing framework and software toolkit which can perform technical tests on regression models for common supervised learning classification and regression models for most of the tabular and image datasets.

AI Verify, however, cannot test Generative AI. To address this, the sandbox was launched to develop evaluation benchmarks for trusted GenAI, anchored on a new draft catalogue proposing a common basis for understanding the current state of large language model (LLM) evaluations.

For a start, (i) key model developers like Google, Microsoft, Anthropic, IBM, NVIDIA, Stability.AI and Amazon Web Services (AWS); (ii) app developers with concrete use cases like DataRobot, OCBC, Global Regulation Inc, Singtel and XOPA.AI; and (iii) third-party testers such as Resaro.AI, Deloitte, EY and TÜV SÜD have joined the sandbox.

Interested model and app developers, and third-party testers are invited to participate in this sandbox.

## GenAI Sandbox for SMEs

In February 2024, Enterprise Singapore (EnterpriseSG) and the Infocomm Media Development Authority (IMDA) [launched the Generative Artificial Intelligence \(GenAI\) Sandbox for small and medium-sized enterprises \(SMEs\)](#).

A curated suite of 13 GenAI solutions will be progressively onboarded to the sandbox by the end of February 2024 to support companies in gaining hands-on experience before deploying them on larger scale.

The GenAI sandbox is expected to benefit some 300 SMEs from sectors including retail, food and beverage, education, and hospitality, which will be able to tap on a range of GenAI solutions to elevate marketing and sales, and customer engagement efforts. Solutions related to marketing and sales, and customer engagement were selected by industry and technical experts from various institutes of higher learning, based on ease of use and deployment for SMEs.

This latest initiative to make available ready-to-use GenAI solutions to local SMEs is part of Singapore's ongoing efforts to collaborate with public and private sectors to accelerate the growth of the AI ecosystem and developments in Singapore.

## ASEAN Guide on AI Governance and Ethics

In February 2024, the Association of Southeast Asian Nations (ASEAN) Secretariat launched the [ASEAN Guide on AI Governance and Ethics](#) (ASEAN AI Guide), which serves as the first common standard in the region that provides guidance on implementing trustworthy AI in ASEAN.

The ASEAN AI Guide provides a framework for organizations within ASEAN countries to design, develop, and deploy AI responsibly. It emphasizes principles such as transparency, fairness, security, human-centricity, privacy, and accountability.

The guide encourages national and regional alignment on AI governance through policy recommendations, and it includes national-level initiatives like nurturing AI talent and investing in AI research, as well as regional-level recommendations like establishing an ASEAN Working Group on AI Governance.

The guide also outlines AI governance structures, human involvement in AI decision-making, and operations management while addressing the need for clear guidelines, ethical standards, and legal compliance to build trust and ensure responsible AI use across the region.

The guide includes AI governance use cases from companies and the public sector in ASEAN. The intention is to help promote consumer confidence and facilitate cross-border deployment of AI-powered services and solutions, enabling ASEAN to fully leverage the power of AI as a region.

## Model AI Governance Framework for Generative AI

In May 2024, AI Verify Foundation and the Infocomm Media Development Authority (IMDA) launched the [Model AI Governance Framework for Generative AI](#) (MGF for GenAI).

This new framework builds on the 2019 Model AI Governance Framework, which was updated in 2020, and covers only traditional AI.

The MGF for GenAI is the first comprehensive framework pulling together different strands of global conversation surrounding AI governance. It outlines nine dimensions to create a trusted environment – one that enables end-users to use GenAI confidently and safely, while allowing space for cutting-edge innovation, namely:

- Accountability;
- Data;
- Trusted development and deployment;
- Incident reporting;
- Testing and assurance;
- Security;
- Content provenance;
- Safety and alignment R&D; and
- AI for public good.

The framework also aims to facilitate international conversations among policymakers, industry, and the research community, to enable trusted development globally. This is the first step towards developing more detailed guidelines and resources under each of the nine dimensions to enable a systematic and balanced approach to AI governance.

The framework will be mapped to international AI principles such as the G7 Hiroshima Principles for interoperability.

## AI Verify Project Moonshot

In May 2024, the AI Verify Foundation launched [AI Verify Project Moonshot](#), an easy-to-use testing toolkit designed to address security and safety challenges often associated with the use of large language models (LLMs).

Project Moonshot is one of the world's first open-sourced tools to bring red-teaming, benchmarking, and baseline testing together in an easy-to-use platform, aimed at addressing the risk of biases and harmful content from unchecked LLMs. It is now available in beta and open-sourced on GitHub, offering developers and data scientists a seamless way to evaluate LLM applications' performance against a baseline of risks, both pre- and post-deployment.

Project Moonshot aims to provide intuitive results of the quality and safety of a model or application in an easily understood manner, even for a non-technical user. It was developed through working with partners such as DataRobot, IBM, Singtel, and Temasek to ensure that the tool is useful and aligned with industry needs.

Project Moonshot is also part of an important move towards global testing standards. Two of the leading AI testing organisations – AI Verify Foundation and MLCommons – have come together to build a common safety benchmark suite.

## AI Playbook for Small States

In September 2024, the world's first [AI Playbook for Small States](#) was launched to shape inclusive global discourse on harnessing the potential of AI.

The AI Playbook is developed by Singapore's Infocomm Media Development Authority (IMDA) in collaboration with Rwanda's Ministry of Information Communication Technology (ICT) and Innovation, with consultations taking place with Digital Forum of Small States (FOSS) members since the start of the 2024.

AI has the potential to uplift individuals, communities and societies, transcending economic value. It in turn plays an important role in contributing to the achievement of all 17 United Nations' Sustainable Development Goals (SDGs). The AI Playbook for Small States aims to build a community of small states and other stakeholders to create the space for inclusive discussions on topics such as AI, allowing small states to tap on its transformative potential.

The playbook is an anthology of experiences of Digital FOSS members on how they have pursued AI adoption and development, considered AI governance and safety, and addressed the societal impact of AI. Some shared challenges include availability of resources and funding, access to data and AI talent, and developing AI governance policies and frameworks. The playbook also offers best practices on how they have implemented AI strategies and policies in their countries.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## ASEAN Guide on Data Anonymisation

The Association of Southeast Asian Nations (ASEAN) has announced that it will be issuing a [new ASEAN Guide on Data Anonymisation](#) in early 2025.

It is intended to serve as an important and practical resource for businesses in ASEAN looking to anonymize data for greater and more responsible use of data across the region.

## AI model risk management for financial institutions

The Monetary Authority of Singapore (MAS) has announced that it will be issuing an [information paper on AI model risk management](#) by Q4 2024/Q1 2025.

This follows another information paper published by MAS on “[Cyber Risks Associated with Generative Artificial Intelligence \(GenAI\)](#)” in July 2024. The paper aims to raise financial institutions’ awareness by providing an overview of key cyberthreats arising from GenAI, the risk implications, and some of the mitigation measures that financial institutions could take to address the risks.

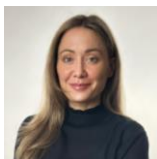
This is part of MAS’s efforts to enable the responsible use of AI in the financial industry. In June 2023, MAS released [Veritas Toolkit version 2.0](#), the first responsible AI toolkit developed specifically for the financial industry to help Fis carry out the assessment methodologies for the Fairness, Ethics, Accountability and Transparency (FEAT) principles.

Veritas Toolkit version 2.0 is available at <https://github.com/veritas-toolkit/>



# Slovenia

## Contacts



**Ana Kastelec**

Managing Partner, Deloitte Legal Reff – branch office in Slovenia  
[akastelec@deloittelegal.si](mailto:akastelec@deloittelegal.si)



**Nika Logar**

Associate, Deloitte Legal Reff – branch office in Slovenia  
[nlogar@deloittelegal.si](mailto:nlogar@deloittelegal.si)

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

## Personal Data Protection Act

The new Personal Data Protection Act (ZVOP-2) came into force in January 2023. ZVOP-2 was adopted with the aim of transposing the GDPR into Slovenian legislation and regulating the effective protection of the right to personal data protection, in line with recent case law from the Court of Justice of the European Union, the European Court of Human Rights, and the Constitutional Court of Slovenia, as well as changes in the legislative field.

Prior to ZVOP-2, personal data protection was governed by the Personal Data Protection Act (ZVOP-1). However, due to the extensive and significant updates required, a new law was necessary to provide effective and transparent regulation, rather than merely amending or supplementing the existing legislation.

ZVOP-2, together with the GDPR, the Act on the Protection of Personal Data in the Field of Criminal Offences (ZVOPOKD), and industry-specific regulations under local laws, comprehensively and systematically regulates personal data protection in Slovenia.

ZVOP-2, specifically and in addition to the GDPR, addresses several areas, such as:

- The use of health, biometric and genetic data;
- The procedures for imposing sanctions and remedies (before ZVOP-2, the supervisory authority lacked sufficient legal basis to impose the sanctions or fines provided under the GDPR);
- The relationship to other legal areas and rights (i.e., access to public information, use of personal data for research, archival and statistical purposes);
- Additional conditions for data protection officers;
- The regulation of video surveillance and audit trace requirements; and

- Other related matters.

Following the adoption of ZVOP-2, the supervisory authority has published several guidelines (e.g., biometrics guidelines, guidelines on the use of cookies and similar tracking technologies) as well as opinions regarding the application of ZVOP-2.

## Biometrics guidelines

The purpose of these guidelines is to explain the basic features of biometric measures, clarify dilemmas related to the processing of personal data in the context of biometric measures, present the new legal framework for these measures under ZVOP-2, and provide answers to the most frequently asked questions from public and private sector entities considering the introduction of biometrics. These include under what conditions biometric measures are permissible, whether this constitutes the processing of personal data, when and how to obtain permission from the Information Commissioner, and other related issues.

Biometric measures, by their nature, represent a significant intrusion into an individual's privacy. Therefore, all conditions for their use must be interpreted in light of privacy protection, based on both the GDPR and ZVOP-2. These regulations establish the rights, obligations, principles, and measures designed to prevent unconstitutional, illegal, and unjustified intrusions into an individual's privacy and dignity during the processing of personal data. Biometrics may only be implemented under the local-specific requirements set out by ZVOP-2, which generally require prior notification to and approval from the supervisory authority.

The guidelines also address the differences between the biometrics regime between ZVOP-1 and ZVOP-2, for example:

- ZVOP-2 no longer restricts the use of biometrics in the private sector exclusively to employees; under certain conditions, biometrics can also be used for clients (e.g., to ensure the accuracy of client identity);
- Employers are no longer required to consult with the representative trade union but must consult with employees regarding the proportionality of the processing;
- Under certain conditions, obtaining prior permission (a decision) from the supervisory authority is no longer mandatory (this applies only exceptionally, as generally, prior permission is required), etc.

### **Judgment of the Administrative Court of the Republic of Slovenia related to direct marketing via telephone**

On 17 January 2023, the Administrative Court of the Republic of Slovenia issued a judgment No. I U 694/2021-19 related to direct marketing via telephone (non-automated calls).

The court explained that the use of automated dialing and communication systems to call a subscriber's phone number without human intervention (e.g., payphones, SMS, MMS), as well as faxes or emails for direct marketing purposes, is allowed only with the subscriber's or user's prior consent. However, this rule does not apply to personal marketing calls, as the law does not require prior consent from the subscriber or user before making such calls.

The law permits the caller to request consent for a marketing call even after the call has been established, provided the subscriber has not already requested a prohibition of marketing calls in advance. If the data subject refuses consent (which must be free of charge), the caller must immediately terminate the call and is prohibited from making further calls to the data subject.

### **Judgment of the Administrative Court of the Republic of Slovenia regarding GPS tracking of company vehicles**

The Administrative Court of the Republic of Slovenia, in its judgment No. III U 267/2022-26 of 18 July 2024, confirmed the decision of the supervisory authority, in which the latter imposed a restriction on the controller's use of GPS tracking of company vehicles, in the sense that it may only collect data from individual locations, but may not carry out systematic, automated and continuous GPS tracking.

The court held that the controller had failed to establish an adequate legal basis for continuous GPS tracking in the inspection procedure and had not demonstrated that such GPS tracking was an appropriate and necessary measure to protect the company vehicles, the equipment and documentation contained therein, to ensure the safety of the employees and to assert and defend against any legal claims.

The court confirmed that the data obtained by the controller through the GPS tracking of company vehicles constituted personal data of the employees, even though the tracking system itself did not record and store the employees' data, but that the employees were identifiable as drivers by means of other documents of the employer (e.g., travel orders). In its judgment, the court also pointed out that it is the controller who must prove the compliance of the processing of personal data in the context of the inspection procedure, referring to the provision of Article 5(2) of the GDPR, which provides that the controller is responsible for compliance with the principles of protection of personal data and must be able to prove such compliance (the accountability principle).



# ? What are the most relevant **cybersecurity updates?**

## **Draft law on the new Information Security Act**

The Office of the Government of the Republic of Slovenia for Information Security (URSIV) has already prepared two drafts on the new Information Security Act (ZInfV-1), which were put up for public consideration. The ZInfV-1 will, among other things, transpose into Slovenian legislation the EU Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the union, also known as the NIS2 directive, which was adopted in December 2022, and EU member states are expected to transpose it into their legal order by 17 October 2024.

Since the scope of the NIS2 directive is much broader than current Slovene legislation, ZInfV-1 introduces several changes for entities already subject to the existing Slovene Information Security Act (ZInfV), requiring them to protect their information systems accordingly. Additionally, many other entities, which will now fall under the new regulation and were not previously obligated, are also expected to face changes, as they have so far reported incidents on a voluntary basis.

ZInfV-1 specifically addresses several key aspects, including:

- The classification of obligated entities into essential and important entities, replacing the former distinction between providers of essential services and digital service providers. The primary difference between essential and important entities centers on their oversight and potential sanctions.
- The requirement for obligated entities to self-register (the establishment of a mechanism for self-registration is envisaged).
- The obligation to report incidents to the relevant authorities without undue delay.

- Obligated entities must implement appropriate and proportionate technical, operational, and organizational measures to manage risks effectively.
- Information security inspectors from URSIV will act as supervisors.
- Control and enforcement measures for obligated entities, such as issuing binding instructions, prohibiting certain actions, mandating the publication of violations of ZInfV-1, and imposing fines.
- Obligated entities are required to perform compliance assessment and self-assessment of compliance regarding the effectiveness of the measures implemented.





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

## **Adoption of act(s) to implement AI Act**

It is not yet known when the acts for the implementation of the AI Act will be adopted or what these acts will entail. Among other things, it will be necessary to specify the supervisory authorities in the act(s) implementing the AI Act.

## **New Media Act to regulate AI use in media**

Slovenia plans to regulate the use of Generative AI in the media by ensuring all media outlets label content created using AI, according to a draft of the new Media Act. If the law is passed, Slovenia will have become one of the first countries to regulate the use of AI in the media by requiring that content in the creation of which Generative AI has been used be labelled appropriately.

Pursuant to a draft of the new Media Act the regulation of AI in media aims to ensure truthful and reliable information, maintain ethical standards, prevent inequality and bias, and safeguard against possible misinformation.

The new Media Act defines both the content entirely created by AI and the parts of content created with AI that journalists include in their articles. The law does not prohibit the use of AI in the media but requires that content in which AI systems have been used is clearly identified and distinctly separated from other media program content. Each program unit, whether text, sound, or audiovisual content, must be clearly labeled.

The draft of the new Media Act is currently in the process of interdepartmental coordination and with the Government Office for Legislation.



# What are the most relevant expected developments in **data protection, cybersecurity and AI?**

## **Personal Data Protection**

There are no specific developments envisaged in the field of personal data protection. As is the case now, the supervisory authority will continue to issue opinions and guidelines that are important for the interpretation of the provisions of the locally applicable data privacy legislation.

## **Adoption of the new Information Security Act (ZInfV-1)**

The Office of the Government of the Republic of Slovenia for Information Security (URSIV) is preparing a new Information Security Act (ZInfV-1), which will, among other things, transpose into Slovenian legislation the EU Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU (NIS2 directive). However, the expected adoption date is not yet clear/determined.

## **Adoption of acts to implement AI Act and adoption of new Media Act**

We anticipate that the acts for implementing the AI Act will be adopted in the future, although the timeline remains uncertain since it is currently unknown whether they are already in preparation or not. Regarding the new Media Act, it is highly likely to be adopted, potentially in 2025. Amendments to the current draft are possible.

# Spain

## Contacts



**Rodrigo González Ruiz**

Partner, Deloitte Legal Spain

[rgonzalezruiz@deloitte.es](mailto:rgonzalezruiz@deloitte.es)



**Carlos de Jorge Pérez**

Senior Associate, Deloitte Legal Spain

[cdejorge@deloitte.es](mailto:cdejorge@deloitte.es)

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

## **Guidelines issued by the Spanish Data Protection Authority (AEPD)**

### **Cookie Use Guide For Audience Measurement Tools - 11 January 2024**

This guideline indicates that, frequently, the use of traffic or performance statistics are essential for the management of a website or app, and that one technical solution is the use of cookies.

By means of this text, conditions are introduced under which type of cookies may be exempt from the user's express consent, provided that a series of requirements are met:

- Its purpose must be exclusively audience measurement;
- The processing must be carried out exclusively on behalf of the publisher;
- They must be used only to produce anonymous statistical data;
- They must not result in the data being matched with other processing operators;
- They must not result in the data being passed on to third parties; and
- They must not allow aggregate tracking of the navigation of the person using different applications or websites.

In order to do so, the publisher must implement several security measures. These include:

- Providing information on the use of these cookies in the privacy policy, and their retention for a maximum period of 25 months; and
- Collecting and processing data separately for each publisher, as well as the cookies used, in case of a provider serving multiple publishers.

### **Cookie Usage Guide - 14 May 2024**

This guide aims to ensure transparency, respect for user privacy, and proper consent mechanisms for the use of cookies:

- **Types of cookies:** Cookies are classified by purpose (e.g., technical, preference, analytics and advertising cookies), duration (session vs. persistent) and whether they are managed by first- or third-party entities.
- **Consent requirement:** For most cookies, especially advertising and analytics, users' explicit consent is required. Websites must provide clear information on cookie usage and allow users to easily accept, reject or manage cookies.
- **Transparency:** Information must be given in layers, with an initial brief notice and more detailed information accessible. Users should be informed about who processes cookies and any possible data transfers.
- **Exceptions:** Some cookies, such as those needed for basic website functionality or security are exempt from consent, but this must be clearly communicated.

The guide stresses the importance of complying with updated regulations in order to build trust in the digital ecosystem.

Lastly, as a novel point, it includes a particular way of requesting the consent of minors.



## Report: Addictive Patterns in the Processing of Personal Data

This [report](#), published in July 2024, highlights how, in many cases, providers implement misleading and addictive design patterns to prolong the time users stay on their services and increase the amount of personal data collected about them.

The AEPD is going to promote that the EDPB includes addictive patterns in the guidelines that are being prepared on the interrelation between the General Data Protection Regulation and the DSA, due to the high impact that these practices have on the right to data protection in digital environments.

The agency's report shows how the processing of users' personal data includes specific operations, all of them deceptive, to influence their decisions and use their personal data for this purpose or to generate new data and perform profiling (referred to in the document as targeting, as it allows for the detailed personalization of addictive strategies).

The paper makes a classification of addictive patterns into three levels:

- High: These are general context- and application-independent strategies, in which four distinct ones have been identified: (i) forced action, (ii) social engineering, (iii) interface interference, and (iv) persistence;
- Medium: They describe more specific approaches that exploit users' psychological weaknesses or vulnerabilities; and
- Low: Correspond to the specific implementation of different approaches and are often context or application specific.

## Sanctions imposed by the AEPD - [PS/00216/2023](#) (2 June 2024)

- The AEPD has sanctioned ENERGYA VM, an energy company with €5 million for breach of the principle of proactive responsibility (Article 5(2) GDPR), and breach of the principle of legality, fairness and transparency (Article 5(1)(a) GDPR).
- ENERGYA VM had contracted the services of a third party (Nivalco) to carry out commercial prospecting work, although this work turned out to be irregular, deceiving clients in order to contract ENERGYA VM's services.
- This canvassing was carried out by illegally extracting data from another energy company (Naturgy). Although ENERGYA VM was warned of the irregularities in the data processing being carried out by Nivalco, the irregularities continued, despite ENERGYA VM taking steps to audit its supplier.
- The AEPD's investigation concluded that (i) no risk analysis was carried out regarding said data processor; (ii) it did not carry out a control of the origin of the personal data; (iii) it did not establish a continuous and exhaustive control of the voice recordings of the hiring process provided by the supplier; (iv) it did not articulate an effective control mechanism over the performance of its data processor despite having evidence that it did not follow its instructions; and (v) it had a reactive rather than proactive attitude.
- ENERGYA VM has ended up paying €2.5 million by receiving deductions for prompt payment.

### Sanctions imposed by the AEPD - [PS/00032/2024](#) (4 December 2024)

- The AEPD fined CAIXABANK, a financial services company, with €2 million for the violation of Article 6(1) GDPR, for processing data without legal basis.
- CAIXABANK requested personal and economic information from the complainant through a form that contained a clause requiring the complainant to give CAIXABANK consent to obtain the complainant's data from the General Treasury of Social Security (TGSS).
- The clause did not offer an option to decline, making the consent preset. After expressing disagreement with this preset consent, CAIXABANK informed the complainant that the clause was standard procedure for all clients and that non-compliance would result in the complainant's bank account being blocked.
- The AEPD noted that because there was no legal requirement for CAIXABANK to verify the personal data information provided by the claimant through the TGSS, CAIXABANK should have first obtained consent from the claimant.
- The AEPD determined that the claimant should have been allowed to withdraw consent without suffering any harm, and the consent should not have been included as a non-negotiable part of the general conditions.
- At the end, after some reductions for early payment, CAIXABANK ended up paying €1.2 million.

### Sanctions imposed by the AEPD - [PS/00424/2023](#) (5 July 2024)

- The AEPD fined with €600,000 a financial entity (4FINANCE SPAIN FINANCIAL SERVICES) for the following infringements: €200,000 for non-compliance with Article 5(1)(f) GDPR (data confidentiality) and €400,000 for non-compliance with Article 32 GDPR (security measures).
- In general terms, the AEPD criticizes the lack of diligence after 4FINANCE notified the supervisory authority with months of delay the existence of a security breach that affected data of consumers and employees, which was not encrypted at all.
- After investigating the facts, the AEPD detected that there was no specific risk analysis of the affected processing activity and that the security measures implement to guarantee identify at login were insufficient.
- Therefore, the principle of data confidentiality was considered to have been violated, considering the combination of personal data subject to the breach, which allowed knowing the financial status of costumers, achieving greater success in the frauds committed, and acting as an aggravating factor, in this case, the late reaction of 4FINANCE, as the anticipation and risk mitigation measures were also insufficient.
- Finally, as the result of some reductions, 4FINANCE paid €360,000.

# ? What are the most relevant **cybersecurity updates?**

## **Guidelines issued by the National Cybersecurity Institute (INCIBE)**

### **New 2024 cybersecurity regulations for vehicles - 13 June 2024**

The purpose of [this guide](#) is to provide information to help understand the new regulation on vehicle cybersecurity issued by the World Forum for Harmonisation of Vehicle Regulations (WP.29), a body of the United Nations Economic Commission for Europe (UNECE), and to provide advice to assist with compliance.

This guide presents the requirements described in both regulations, along with recommendations and guidance on how to properly comply with them and which internal processes of manufacturers and suppliers may be affected by the new regulations.

This regulation consists of two regulations, R155 and R156, which set out the cybersecurity requirements that manufacturers must meet in order to qualify for type approval of vehicles for sale in countries of the European Union or countries outside the EU that adopt these regulations. In particular, these two regulations deal with the following issues:

- R155 deals with cybersecurity management requirements; and
- R156 deals with software update management requirements.

In Spain, these requirements will be mandatory for all vehicles from 1 July 2024, affecting not only the vehicles themselves, but also the operations of manufacturers and suppliers.

## **Study of malware analysis in SCI: BlackEnergy - 2 February 2024**

This [study](#) shows the evolution of cybersecurity and the changes made to industrial environments as a result of cyberattacks, with the aim of preventing them from happening again. In particular, this guide contains:

- It begins with a historical review that shows the evolution from its appearance to the latest version detected, which allows us to see how it has affected industry, analyzing the reasons for its success.
- The second part of the study focuses on the different types of analysis possible, the preparation of the environment and the different types of tools that allow this to be done.
- Finally, an example of a detailed technical analysis of a sample is given, describing the steps involved, including the creation of a secure environment, the installation of the software, and the use of commands to extract as much information as possible from it.



## **Guidelines issued by the National Cryptology Centre - Computer Emergency Response Team (CCN - CERT)**

### **Cybersecurity Risk Observatory - April 2024**

This [report](#) presents a Cybersecurity Risk Observatory that, while having a broad and general perspective, is primarily oriented towards the public sector. The report identifies 17 risks, organized into the following seven thematic areas:

- Technological developments;
- Sociopolitical;
- Criminality structure;
- Institutional;
- Organizational culture;
- Sectoral; and
- Resources.

In this regard, the report provides a description of the risks identified in each area of concern, as well as the risk level of each of these risks. In addition to this, it also includes a chapter of:

- Summary of the incident;
- Parties involved in the incident;
- Description of the incident;
- Relationship of the incident to the center's risks;
- Consequences; and
- Lessons learned.

## **Data Protection in the Cloud: Digital Sovereignty - May 2024**

This [guide](#) aims to provide an updated overview, together with some recommendations, of the technological solutions and resources typically offered by cloud service providers (CSPs), as well as to review the state of the art of hyperscale providers' technology and solutions to ensure digital sovereignty, including aspects related to data confidentiality, integrity and availability.

To this end, the guide describes the different technical, organizational and contractual measures that CSPs must comply with in order to mitigate the risk scenarios associated with this type of solutions. The risks described cover different scenarios related to logical and physical security, privacy, as well as certain regulatory aspects applicable in the European Union.

Without being an exhaustive guide, it is intended as a reference document so that technical and business leaders can find the necessary balance to innovate and, at the same time, comply with security requirements in the cloud.





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

## Spanish's Artificial Intelligence Strategy 2024 - 5 June 2024

The strategy will run from 2024-2025. It is a plan to develop and expand the use of artificial intelligence in a transparent and ethical manner and focuses on facilitating its use in the public and private sectors.

The [Artificial Intelligence Strategy 2024](#) focuses on three key areas:

- **Strengthening the use of AI across the economy:** The government is committed to strengthening capabilities to meet the growing demand for artificial intelligence products and services in four areas: supercomputing, cloud infrastructure, AI language models and talent needs.
- **Facilitate the application of AI in the public and private sectors:** The public sector should drive the application of AI to improve service delivery to citizens and serve as a catalyst for change in the private sector. To this end, the General State Administration will promote AI pilot projects and innovative solutions through an innovation laboratory. It will also develop a common data governance model. To promote the development of AI in the private sector, the government has already launched the Kit Consulting program and expanded the Kit Digital program.
- **Promoting transparent, accountable and humanistic AI:** The aim is to achieve a broad social consensus on the uses of artificial intelligence, its limits and the way people interact with AI developments. Spain, through the Spanish AI Supervisory Agency (AESIA), created in August 2023, aims to lead the use of responsible, safe and ethical artificial intelligence, establishing a governance framework that ensures the highest levels of transparency and trust.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## A Coruña to be home to Spain's AI Supervisory Agency

The council of ministers adopted the decision that A Coruña will be the headquarters of the Spanish Agency for the Supervision of Artificial Intelligence, after passing the objective and technical process of assessing the candidatures presented, in line with the commitment to decentralization of the government's public sector and the structuring of the territory. With this decision, Spain becomes the first country in the European Union with a Spanish Agency for the Supervision of Artificial Intelligence, prior to the entry into force of the future European regulation, which establishes the need for member states to have a supervisory authority in this area.

The agency will be located in Galicia, making this region a pole of attraction and retention of qualified talent, helping to combat the phenomenon of depopulation and generating direct and indirect employment.

It will be responsible in Spain for overseeing the development of a respectful and safe ecosystem for the use of this technology and will strengthen the research, business and social ecosystem related to this field.

The recruitment of highly specialized AI professionals to staff the Secretariat General and the heads of division of AESIA will begin shortly. This will be followed by the approval of the staff structure and the selection process for officials and staff.

## Transposition of the NIS2 Directive in Spain

17 October 2024 is the deadline for member states to transpose the NIS2 Directive on measures to ensure a high level of cybersecurity into their national legislation. In Spain, the process of transposing this directive into Spanish law continues, although there is still no draft of the future legislative text.

# Sweden

## Contacts



**Lisa Bastholm**

Senior Manager, Deloitte Legal Sweden

[bastholm@deloitte.se](mailto:bastholm@deloitte.se)



**Michelle Smed**

Assistant Manager, Deloitte Legal Sweden

[msmed@deloitte.se](mailto:msmed@deloitte.se)

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

## **Use of the Meta-Pixel resulted in unlawful transfer of sensitive data**

The Swedish Authority for Privacy Protection (IMY) have investigated two Swedish pharmacies in relations to the use of Meta-Pixel (formerly called Facebook-Pixel). By activating a new function of Meta-Pixel, the companies transferred sensitive personal data to Meta, including contact information and details regarding the customer's purchases of over-the-counter medications, treatments, and self-administered tests of specific medical conditions.

According to the IMY investigation, the companies did not use or implement any technical measures to control and limit the transfer of data to Meta, and they did not have sufficient safety measures or routines in place. The transfer of data occurred over a long period of time and was discovered by external reports. IMY stated that the two pharmacies failed to implement sufficient technical or routine safety measures, and thus the transfer of data to Meta violated the GDPR.

IMY indicated that, processing this type of privacy-sensitive personal data involves high risks that entail requirements for a high level of protection. The companies had an obligation to take appropriate measures to protect the data from, for example, being shared with unauthorized persons.

The two pharmacies were fined SEK 37 million and SEK 8 million respectively. Two investigations regarding a third Swedish pharmacy as well as a Virtual Healthcare Provider in relation to their use of the Meta-Pixel are currently ongoing.

## **Requirements for accreditation of certification bodies established**

The Swedish Authority for Privacy Protection (IMY) has finalized the requirements for accreditation of certification bodies. The requirements are to be applied by the Swedish national accreditation body, Swedac.

According to the IMY, the certification makes it easier for companies and other organizations to comply with the GDPR and is a way to demonstrate that a certain type of personal data processing is lawful. IMY's decision now makes it possible for certification bodies to issue certificates in Sweden as it relates for example to certificates for personal data processing throughout the EEA (so called EU data protection seals) or certificates for personal data processing that primarily take place in Sweden.

The certificates are to be issued in accordance with certification schemes approved by the competent supervisory authority or the European Data Protection Board which guarantees a high level of data protection for the personal data processes that are certified.

The application for accreditation is to be submitted directly to Swedac. Any request to have a certification scheme approved is sent to IMY.



## Review of DPO roles completed by IMY

In March 2023, the European Data Protection Board (EDPB) along with several national data protection authorities launched a coordinated action to assess if the roles of data protection officers (DPO) meet the requirements of Article 37 and Article 39 of the GDPR and if they have the resources needed to carry out their tasks.

According to the report from EDPB, the majority of the businesses surveyed believed that the DPO's have the necessary skills and knowledge to carry out their work and receive regular training on data protection issues, that they have clearly defined tasks and that they are not pressured on how to carry out these tasks.

The Swedish Authority for Privacy Protection (IMY) decided to continue the work by conducting an in-depth review of several national organizations. One of the aspects IMY reviewed was how DPO's manage conflicts of interest.

According to the GDPR, certain businesses are obliged to appoint a DPO. The role of the DPO is to help ensure that operations comply with data protection legislation. A DPO may work with other tasks and assignments in addition to the data protection work, provided that it does not lead to a conflict of interest.

The IMY found that the role of one DPO violated the GDPR as the DPO's additional role as legal counsel created a conflict of interest when reviewing the organization's compliance with the data protection rules as this included the review of the management team, to which the DPO also provided legal advice. A second reprimand was issued to an organization for not ensuring that the DPO correctly, and in a timely manner participated in all matters related to the protection of personal data, not providing the DPO with the required resources and not ensuring that the DPO reported directly to the organization's highest administrative level.

## GDPR versus the constitutional right to freedom of speech

According to the Freedom of Speech Act (1991:1469), it is possible for anyone to apply for a voluntary "publishing license", granting a database constitutional protection under the Freedom of Speech Act. When the Freedom of Speech Act applies, GDPR has not been applicable as a general rule. In practice, publishing licenses has therefore been used by webpage providers to avoid the applicability of GDPR. In Sweden, there are many providers of webpages which collect information about natural persons and publishes it in a searchable format. Such data can include address, financial status and criminal offences. Previously, it has not been possible for data subjects to use their GDPR rights against such websites with a publishing license, as it would be intrusive on the freedom of speech.

In the decision by the Administrative Court of Appeal, a company had requested personal data from the Public Prosecution Service, presenting a so-called voluntary publishing license from the Swedish Press, Radio and Television Authority (now the Swedish Media Authority) and stated that the personal data was needed for future journalistic activities. In previous contacts with the Public Prosecution Service, the company had said that it carried out background checks and recruitment consultancy. The Swedish Prosecution Authority rejected the request because it considered that it had not been established that the journalistic purpose of the processing was the main purpose and that the Swedish exemption from the application of the EU Data Protection Regulation for journalistic activities was therefore not relevant.

Taking into account the primacy of EU law and the case law of the Court of Justice of the European Union, the Court of Appeal considered that a balance must be struck between the interest in protecting privacy and the constitutionally protected rights of holders of voluntary publishing licenses. In striking such a balance, the Administrative Court of Appeal considered in this case that the GDPR applied and that the rights of the data subjects weighed more heavily.

# ? What are the most relevant **cybersecurity updates?**

## **New legislation proposed for the implementation of the NIS2 Directive**

The NIS Directive from 2016 was incorporated to Swedish law through the Act (2018:1174) on Information Security for Essential and Digital Services (NIS). As a result of the NIS2 Directive, new Swedish legislation is proposed, The Cyber Security Act, and is suggested to replace the previous Act (2018:1174).

The NIS2 Directive imposes additional requirements for operators and provides more far-reaching cooperation within the EU. The aim is to achieve a higher level of cybersecurity.

There are two key differences between the current Swedish legislation and the proposed Cyber Security Act. First, the Cyber Security Act is suggested to cover significantly more actors, as the number of sectors is increased from seven to 18. The other important difference is that the requirements will apply to the entire business, not just to essential and digital services.



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

## **Nordic collaboration on AI and children's rights**

**At the annual Nordic Data Protection Meeting, the Swedish Authority for Privacy Protection (IMY), together with the other Nordic data protection authorities, adopted a declaration on measures to deepen the Nordic cooperation.**

At the meeting, the data protection authorities agreed on a set of common principles related to children and online gaming. The principles, which will be published shortly, sets out how game developers are to protect children's rights.

Regarding AI, the Nordic data protection authorities noted that even though the upcoming AI regulation aims at certain aspects of AI, the General Data Protection Regulation (GDPR) still applies to the processing of personal data. Most things related to the development, training and use of AI will involve the processing of personal data. Therefore, both the AI regulation and GDPR will affect the use of AI.

It is now important for the Nordic data protection authorities to assess future resource needs in order to be able to provide guidance on AI and ensure that there are no uncertainties about which legislation applies.

## **First interim report from pilot project on AI regulatory sandbox published**

**The Swedish Authority for Privacy Protection (IMY) is participating in a joint pilot project that aims to increase knowledge about how AI regulatory sandboxes should operate in Sweden. The first insights are now published in an interim report.**

The IMY, together with the Swedish Companies Registration Office, the Swedish Tax Agency and the Swedish Public Employment Service, have started a pilot project of an AI regulatory sandbox. The AI regulation requires a sandbox in each member state where AI systems can be trained and tested in a controlled environment before they are put into use.

Some of the insights that have emerged are the following:

- It can be complicated to draw the boundaries of the scope of an AI system, i.e., what is part of the system and what is not. The intended purpose of the system should be at the center.
- A key issue is to identify the level of risk an AI system belongs to. This is particularly important if the system is a so-called high-risk system, because of the special requirements placed on these systems.
- A cross-functional approach is crucial. A smaller working group that is active provides better collaboration. The continuous documentation is important in order to be able to go back to previous reasoning.



## What are the most relevant expected developments in data protection, cybersecurity and AI?

### **IMY comments on proposed changes to the regulation surrounding the use of video surveillance**

**New legislation that strengthens the police force's rights to use video surveillance and technology for automatic facial recognition has been proposed.**

The Swedish Authority for Privacy Protection (IMY) is now commenting on the proposal and emphasizes that additional regulations are required to limit the invasion of privacy in order for the proposals to meet the requirement of proportionality.

The IMY indicates that while it is important that the police force is provided better tools and measures to fight organized crime, it is imperative to ensure people's right to privacy. In its statement, IMY highlights that the proposal for expanded opportunities for camera surveillance risks enabling a general collection of data on individuals' movements throughout the country. IMY therefore believes that further regulation is needed to limit this risk.

The IMY states that “it would be possible to give the police better opportunities for camera surveillance, but further measures are needed to protect personal integrity. Our assessment is that the current proposal does not meet the requirement for a balance between the interest in law enforcement and the protection of privacy”.

The Ministry of Health and Social Affairs also agreed with the IMY in that supplementary regulations are required to protect the personal integrity of individuals and other fundamental rights and freedoms with regard to automatic facial recognition in public places. Only when there are proposals for such supplementary regulations is it possible to assess whether the proposal meets the requirement of proportionality.



# Switzerland

## Contacts



**Paul de Blasi**

Partner, Deloitte Legal Switzerland  
[pdeblasi@deloitte.ch](mailto:pdeblasi@deloitte.ch)



**Audrey Soutter**

Senior Manager, Deloitte Legal Switzerland  
[asoutter@deloitte.ch](mailto:asoutter@deloitte.ch)

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

## **Switzerland ratifies the Convention 108+**

**Switzerland ratifies the only legally binding instrument for the protection of personal data and the right to privacy at an international level**

On 7 September 2023, Switzerland adopted the modernised Convention on Data Protection of 1981 (the so-called Convention 108) by ratifying the Amending Protocol (the so-called Convention 108+), which is intended to respond to the challenges linked to the use of new technologies. For the Convention 108+ to enter into force, the Amending Protocol must be ratified by the 38 states parties. The Federal Data Protection and Information Commissioner's publication with additional information is available [here](#).

## **The Freedom of Information Act: two recommendations**

**Recommendations on contracts for COVID vaccines and the takeover of Crédit Suisse by UBS published in November 2023**

During the recent pandemic, there were several applications before the Federal Office of Public Health to access contracts for COVID-19 vaccines, ultimately leading to mediation requests submitted to the Federal Data Protection and Information Commissioner. This latter considered that access to these contracts should be granted to a large extent. The relevant publication with additional information is available [here](#).

In the context of the Crédit Suisse takeover, there were several applications for access to information before the General Secretariat of the Federal Department of Finance and the State Secretariat for International Financial Matters. The Federal Data Protection and Information Commissioner recommends deferral of access until investigations are concluded; the analysis of the situation with additional information and links to the recommendations is available [here](#).

## **The current data protection legislation is directly applicable to AI**

**The Federal Data Protection and Information Commissioner confirms that the Federal Data Protection Act covers AI-supported data processing**

Considering the recent developments in the US and the EU, the Federal Data Protection and Information Commissioner published in November 2023 a statement regarding the applicability of the Federal Data Protection Act to AI-supported data processing. He recalled that the obligations contained in the Act must be complied with independently of whether data is processed by human beings or AI. The Federal Data Protection and Information Commissioner's publication with additional information is available [here](#).

We include further details in the most relevant AI updates slides.

## **EU adequacy decision regarding Switzerland**

**Personal data from EU/EEA states can continue to be transferred to Switzerland without additional guarantees**

On 15 January 2024, the European Commission confirmed that Switzerland offers an adequate level of protection for the processing of personal data. While an adequacy decision was in place for Switzerland since 2000, it had been issued under the precursor to the currently applicable General Data Protection Regulation (the so-called GDPR). This decision confirms that Switzerland's new data protection legislation meets the adequacy requirements under the GDPR.

The Federal Data Protection and Information Commissioner's publication with additional information and a link to the European Commission's decision is available [here](#).

## Guide to Technical and Organisational Data Protection Measures

**An updated version of the guide is available, along with an English language version**

In January 2024, the Federal Data Protection and Information Commissioner published an updated Guide to Technical and Organisational Data Protection Measures, dealing with concepts such as encryption, anonymisation, or authentication. It is intended to be used as an aid with implementation of appropriate measures ensuring optimal and appropriate protection of personal data.

The Federal Data Protection and Information Commissioner's publication with additional information and a link to the Guide is available [here](#).

## Factsheet on planning and justifying online access

**Online access must be planned in accordance with the requirements of the Federal Act on Data Protection**

Online access, i.e., online disclosure of personal data between different authorities on a self-service basis, is imposed by numerous laws. Being susceptible to causing serious prejudice to data subjects' fundamental rights, such access must be planned by federal bodies in good time and in line with the underlying principles of the Federal Act on Data Protection. As the Federal Data Protection and Information Commissioner noted, it is not sufficient to justify online access simply by reference to the need for digitalization of public administration.

The Federal Data Protection and Information Commissioner's publication as well as the factsheet are available [here](#).

## New Swiss-US Data Privacy Framework

**New agreement ensuring adequate data protection for the secure exchange of personal data between Switzerland and certified US companies**

Since July 2023, the EU and the US have been operating under the EU-US Data Privacy Framework when it comes to transfer of personal data (see the relevant publication on the Federal Data Protection and Information Commissioner's website [here](#)). With the new Swiss-US Data Privacy Framework coming into force on 15 September 2024, the Swiss Federal Council has leveled the playing field for individuals and businesses operating in Switzerland.

The Swiss-US Data Privacy Framework in a nutshell:

- Based on an assessment by the Federal Office of Justice (available [here](#)), the Swiss Federal Council considers that the Swiss-US Data Privacy Framework provides adequate protection for secure exchange of personal data between the two countries; as such, personal data can now be transferred from Switzerland to certified US companies without any additional guarantees.
- In force as from 15 September 2024 via an amendment to the Data Protection Ordinance.
- The list of US companies certified under the Swiss-US Data Privacy Act is available [here](#); the website also contains information regarding the EU-US Data Privacy Framework.
- To benefit from the Data Privacy Framework Program (which includes not only the Swiss-US Data Privacy Framework, but also the EU-US Data Privacy Framework and its UK extension), the interested US-based organizations must self-certify and then annually re-certify to the US Department of Commerce's International Trade Administration that they adhere to the relevant Data Privacy Framework Principles and develop a compliant privacy policy.



# ? What are the most relevant **cybersecurity updates?**

## **The national strategy for Switzerland's protection against cyber risks**

**A project aimed at research providing data, insights and recommendations, with a special focus on non-technical aspects of cybersecurity**

Between 2021 and 2024, the project, which is a part of the Swiss National Science Foundation's National Research Program 77 "Digital Transformation", is to fund two doctoral theses, as well as various scientific publications and conferences. Further information about the project, which is now nearing completion, is available [here](#).

In December 2023, the CERTs and Ethics Guidelines were published in the context of the project, seeking to create a value-driven cybersecurity culture (available [here](#)).

## **FINMA Annual Report 2023**

**Deficiencies around governance and identification of potential threats; higher cyber risks associated with outsourcing**

In its Annual Report 2023, the Swiss Financial Market Supervisory Authority (FINMA) concluded that:

- The number of cyberattacks remained stable when compared to those recorded in 2022;
- There are deficiencies in the area of governance and the identification of potential threats, including but not limited to an unclear boundary between the first and second lines of defence, deficiencies in identifying potential institution-specific threats, along with shortcomings in the protective measures regarding data loss prevention; and
- Outsourcing is associated with higher cyber risks.

The report is available [here](#), with FINMA's accompanying publication [here](#). The risk of cyberattacks is also assessed in the FINMA Risk Monitor 2023, available [here](#).

## **The Swiss Information Security Act**

**The Information Security Act entered into force on 1 January 2024; a revision is scheduled to enter into force on 1 January 2025**

On 1 January 2024, the Information Security Act and the associated ordinances, dealing with the information security of the federal government, entered into force. An updated version, including an obligation to report cyberattacks where critical infrastructure is involved, is scheduled for 1 January 2025.

## **Xplain hack: data analysis report**

**The National Cyber Security Centre published its report**

Xplain, a major provider of IT services, was affected by a hacker attack which resulted in data being published on the darknet in June 2023. The stolen data included classified information and sensitive personal data from the federal administration.

The National Cyber Security Centre reported on the procedure and the results of the analysis of the leaked data. Its publication with a link to the report is available [here](#).

## **FINMA's Guidance 03/2024 on cyber risks**

**Findings by FINMA regarding cyber risks, including details on the obligation to report cyber attacks and scenario-based cyber risk exercises**

In June 2024, FINMA published its Guidance 03/2024, which includes its cyber risk supervision findings and clarifies the FINMA Guidance 05/2020. Consistently with its other publications, it identifies outsourcing as a risk driver, alongside other topics, including governance.

FINMA's press release is available [here](#), along with the Guidance 03/2024 [here](#).





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

## **Meta will not change its terms of use for Swiss users**

### **Facebook and Instagram data will not be used to train Meta's AI**

Meta had originally announced that it would start using data of adult users for AI training as of June 2024 but suspended the project in advance for the EU/EEA countries. It further expressly confirmed to the Federal Data Protection and Information Commissioner that data of users in Switzerland will not be used for AI trainings either.

The Federal Data Protection and Information Commissioner's publication on this topic is available [here](#).

## **FINMA Risk Monitor 2023 looks at challenges in connection with AI**

### **AI classified as a trend with the potential to affect the Swiss financial market over long term**

FINMA's yearly Risk Monitor report provides an overview of the most important risks that supervised institutions are faced with. Among the nine main risks contained in the Risk Monitor 2023 is the risk of cyberattacks. Aside from the main risks, each Risk Monitor focuses on a trend which has the potential to affect the Swiss financial market over the long term. Being increasingly important in various areas of life, FINMA considers the use of AI as being a trend that fits the above definition. In particular, the Risk Monitor considers the challenges associated with the responsibility for AI decisions, the reliability of AI applications, the transparency and explainability of AI decisions and the equal treatment of financial market clients and expects supervised institutions to respond to these and the associated risks appropriately.

The Risk Monitor 2023 is available [here](#), with FINMA's accompanying publication [here](#).

## **The current data protection legislation is directly applicable to AI**

Considering the recent developments in the US and the EU, the Federal Data Protection and Information Commissioner published in November 2023 a statement regarding the applicability of the Federal Data Protection Act to AI-supported data processing. They recalled that the obligations contained in the act must be complied with independently of whether data is processed by human beings or AI.

In this context, the relevant stakeholders must:

- Ensure that in the development and use of new technologies, data subjects have the highest possible degree of digital self-determination;
- Render the purpose, functionality and data sources of AI-based processing transparent, so as to enable data subjects to exercise their right to object to automated data processing or to request that automated individual decisions be reviewed by a human being;
- Inform the users of whether they are communicating with a machine (i.e., an intelligent language model) and whether the data they enter is being processed to improve self-learning programs or for other purposes;
- In the same vein, clearly indicate the use of programs that enable the falsification of faces, images or voice messages of identifiable persons; the use of such programs may be unlawful in specific scenarios under criminal law; and
- Take appropriate measures, including a data protection impact assessment, where AI-supported data processing involves high risks; any applications undermining the privacy and informational self-determination are prohibited.

The Federal Data Protection and Information Commissioner's publication with additional information is available [here](#).



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Swiss electronic identity (e-ID) will be optional from 2026

### Federal, optional and free – the three adjectives defining the upcoming Swiss e-ID

On 10 September 2024, the Council of States adopted the draft bill for the Swiss electronic identity. A few open points remain with respect to the individual data protection and cybersecurity issues – these will be settled by the National Council.

The press release of the Swiss parliament is available [here](#) (only in German).

## Potential Swiss AI regulatory framework proposal

### Federal Council examines regulatory approaches to AI

In 2019, the State Secretariat for Education, Research and Innovation (SERI) issued a report prepared by an interdepartmental working group under SERI's guidance to the Federal Council, concluding that there was no immediate need for Switzerland to introduce AI-specific legislation. In 2020, the Federal Council adopted the Guidelines on Artificial Intelligence for the Confederation, prepared by the same interdepartmental working group, a document applicable to the federal administration. Further information can be found on the [SERI website](#).

In 2023, recognizing the global trend of regulating AI, the Federal Council mandated the Department of the Environment, Transport, Energy, and Communication to prepare a report on possible approaches to AI regulation by the end of 2024, with the aim of having a potential AI regulatory framework proposal in the course of 2025. The analysis is to build on existing Swiss legal framework and ensure the approaches are compatible with the EU AI Act and the Council of Europe's AI Convention, both of which are relevant for Switzerland (see below). The Federal Council's press release is available [here](#).

In the meantime, the relevant stakeholders must comply with existing legislation, including but not limited to the Federal Act on Data Protection. Moreover, the EU AI Act, which came into force on 1 August 2024, has a broad territorial scope, thus impacting likely not only EU providers and deployers, but also non-EU stakeholders, especially where these develop AI systems supplied to EU-based entities and/or deploy AI systems with output used in the EU, for example by clients or customers residing there.

# Thailand

## Contacts



**Anthony Visate Loh**

Partner, Deloitte Legal Thailand

[aloh@deloitte.com](mailto:aloh@deloitte.com)



**Sutthika Ruchupan**

Director, Deloitte Legal Thailand

[sruchupan@deloitte.com](mailto:sruchupan@deloitte.com)



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

## **The Master Plan for the National Promotion and Protection of Personal Data**

On 5 April 2024, the Office of the Personal Data Protection Committee, with the approval of the Personal Data Protection Committee (PDPC) and the National Digital Economy and Society Commission, issued the Master Plan for the National Promotion and Protection of Personal Data.

The master plan identifies the strengths, weaknesses, opportunities and threats faced by Thailand's current approach to personal data protection. The master plan outlines the relevant policies, national strategies and plans as well as set out the objectives and key success identifiers. The master plan outlines the objectives for the four-year span of the plan, from 2024 to 2027, as well as set out the four strategies to achieve the objectives under the following headings:

- PDPA Effective and Balanced Enforcement;
- PDPA Knowledge and Trust Enhancement;
- PDPA Digital Economy and Society Promotion; and
- PDPA R&D and Technology Adoption.

The master plan further sets out the key drivers of each of the relevant policies, national strategies and national plans, spanning from implementing the master plan through existing regulators and the appointment of advisors across different sectors, and seeking cooperation from the local to the international level, as well as through management of human resources, government budgets, monitoring of progress and undertaking of relevant assessments.

## **The Prescription of Subordinate Laws by the Personal Data Protection Committee**

In 2024, the PDPC has introduced a number of new legislations to further clarify the enforcement of the Personal Data Protection Act (PDPA).

A summary of the PDPC's newly introduced legislation in 2024 are provided below.

### **Summary of PDPC Legislation 2024**

- Notification of the Personal Data Protection Committee Regarding the Criteria for the Prescription of Administrative Penalties by the Expert Committee (No. 2), B.E. 2567 (2024) (PDPC Notification on Administrative Fines).
  - PDPC Notification on Administrative Fines amended the provision of the PDPC Notification regarding the Criteria for the Prescription of Administrative Penalties by the Expert Committee B.E. 2565, which relates to the prescription of administrative penalties for serious offences under the PDPA. The amendment removed the reference to the PDPC's regulation on the prescribed rate of penalty, thus offering more flexibility to the expert committee.
- Notification of the Personal Data Protection Committee Regarding the Criteria for Deletion, Destruction, or Anonymization of Personal Data to Render it Unidentifiable to the Data Subject, B.E. 2567 (2024) (PDPC Notification on Erasure).
  - The PDPC Notification on Erasure requires provides, among other things, for data controllers to respect the data subject's right to request for the erasure, destruction or anonymization of personal data within the prescribed time frame.



- Data controllers must ensure the methods employed for the erasure, destruction or anonymization of personal data are consistent with the specifications and criteria set out in the PDPC Notification on Erasure.
- Notification of the Personal Data Protection Committee Regarding the Criteria for Protective Measures for the Collection of Personal Data Related to Criminal Records Not Conducted Under the Control of Authorized Legal Authorities, B.E. 2566 (2023) (PDPC Notification on Criminal Record Protective Measures)
  - This notification sets out the circumstances in which a data controller may collect a data subject's criminal record as well as specific obligations of data controllers in relation thereto.
  - A data controller may collect criminal records only if required to do so by law, or where explicit consent is obtained provided it is for the specified purposes. For example, for the purposes of employment or assessment of qualifications, suitability or prohibited characteristics.
  - Under the PDPC Notification on Criminal Record Protective Measures, data controllers are obligated to put in place appropriate security measures, including organizational measures, technical measures, and physical measures to safeguard the criminal record.
  - Unless otherwise required by law, or consent is obtained, a data controller may not retain the criminal record for more than six months after the data controller has processed such criminal records for the lawful purpose.

- Notification of the Personal Data Protection Committee Regarding the Criteria for the Protection of Personal Data Sent or Transferred Abroad According to Section 28 of the PDPA B.E. 2566 (2023) (Section 28 Notification)
  - On 25 December 2023, the PDPC introduced the Section 28 Notification, which sets out, among other things, the criteria for personal data recipient countries to be deemed to have adequate standards of personal data protection, which would accordingly permit data controllers to transfer data to such countries in accordance with the PDPA.
- Notification of the Personal Data Protection Committee Regarding the Criteria for the Protection of Personal Data Sent or Transferred Abroad According to Section 29 of the PDPA B.E. 2566 (2023) (Section 29 Notification)
  - The Section 29 Notification issued by the PDPC on 25 December 2023, elaborates on the requirements for binding corporate rules (BCR) which if approved by the PDPC, data controllers can rely on when undertaking cross-border data transfer within a conglomerate.
  - During the time while there are no BCRs or rulings on countries approved by the PDPC, cross-border transfer of personal data remains permissible through the implementation of "appropriate safeguards", which for the private sector can take the form of either (i) standard contractual clauses (SCC), or (ii) certifications that adhere to the criteria specified in the up-coming PDPC notification.

## **The PDPC fines a Thai business operator in the computer retail industry 7 million Baht**

In August 2024, a Thai company operating business in the retail of computers and computer parts has been fined by the expert committee for the failure to:

- Appoint a data protection officer with the prescribed time;
- Put in place appropriate security measures to protect the personal data of its customers; and
- Notify the breach to the PDPC and the relevant data subjects as required by the PDPA.

The company was subject to a total fine of 7 million Baht, which was the aggregate total of the maximum fine imposable under each offence and was required to take immediate rectification actions and report to the PDPC in accordance with the prescribed time frame.

This marks one of the first publicized cases which the PDPC has imposed such enforcement action on a data controller in Thailand.



# What are the most relevant expected developments in **data protection, cybersecurity and AI?**

## **The Master Plan for the National Promotion and Protection of Personal Data**

### **AI governance, law and regulation**

Thailand does not currently have specific regulations on AI, however, based on the master plan, there are plans to introduce legislation to regulate the use of AI in the near future.

As Thailand moves towards integrating AI into its economy, the government realizes the necessity of having a clear regulatory framework, prescribed standards, as well as policies to support this movement.

As such, part of the National Artificial Intelligence Action Plan for the Development of Thailand (2022-2027) under the broader Policy and National Plan for Digital Development for the Economy and Society (2018-2037) of the master plan, and in order to prepare Thailand for the incorporation of AI, the formulation of policies, guidelines, regulations, standards, and legislation of related laws are underway.

## **Subordinate laws of the Personal Data Protection Act**

### **Further PDPA development**

Notwithstanding the numerous subordinate laws issued by the PDPC in the past few years, there remains a number of subordinate laws which have yet to be issued by the PDPC.

For example, the implementation of “appropriate safeguards” by way of certification pursuant to the Section 29 Notification, in which it provides that certification shall be in accordance with the specifications of the PDPC. It is therefore expected that subordinate laws will be issued in the upcoming years to further complement the PDPA.

In addition, given that the PDPA is still relatively new, it is expected that the PDPC will continue to publish guidelines and handbooks to enable stakeholders across all sectors to comply with the provisions of the PDPA.

# The Netherlands

## Contacts



**Sebastiaan ter Wee**

Partner, Deloitte Legal Netherlands

[sterwee@deloitte.nl](mailto:sterwee@deloitte.nl)



**Marlieke Bakker**

Senior Manager, Deloitte Legal Netherlands

[mabakker@deloitte.nl](mailto:mabakker@deloitte.nl)



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

## **Global ride-hailing company fined**

The Dutch DPA has fined a global ride-hailing company €10 million for failing to provide sufficient transparency about how long it retained personal data of European drivers and to which countries outside Europe this personal data was transferred. The company also made it difficult for drivers to exercise their data subject rights. (December 2023)

## **Doxing declared illegal in the Netherlands**

As of 1 January 2024, doxing is illegal in the Netherlands. Doxing can be defined as ‘providing, distributing or otherwise making personal data available with the intention of intimidating someone’. Often, journalists, politicians, and other public figures are targeted. Dutch criminal law allows for fines and imprisonment up to two years, with higher penalties for targeting specific professionals. (January 2024)

## **Credit card company fined for missing risk assessment**

The Dutch DPA has fined a credit card company €150,000 for using customers' personal data on a large scale without conducting a legally required Data Protection Impact Assessment (DPIA), which assesses potential privacy risks. By failing to perform this assessment, the company violated the GDPR. (January 2024)

## **DPA intensifies checks on cookie consent compliance**

The Dutch DPA has announced plans to increase inspections in 2024 to verify that websites are correctly obtaining consent for tracking cookies and other tracking software. It offers clear guidelines on its website, outlining how organizations should design cookie banners to properly request consent. The DPA notes that, in practice, many organizations use deceptive cookie banners, such as hiding certain buttons. (February 2024)

## **Company fined for illegal data collection for facial recognition**

The Dutch DPA has fined a facial recognition company €30.5 million and imposed additional penalties with a maximum of over €5 million. The company offering facial recognition services to intelligence and law enforcement agencies has illegally created a database containing billions of facial images, including those of Dutch citizens. The company is based in the United States and does not have an establishment in Europe. Although the company has been fined by other data protection authorities before, it does not seem to adapt its conduct. The Dutch DPA is now investigating if the directors of the company can be held personally responsible for violations. (May 2024)

## **Company fined for unlawful use of tracking cookies**

The Dutch DPA has imposed a fine of €600,000 on a major health and beauty retailer. The fine was issued because the company tracked visitors on its website using tracking cookies without the users' knowledge and proper consent. As a result, the company unlawfully collected and used sensitive personal data from millions of website visitors. (May 2024)

## Dutch DPA declares web scraping nearly always illegal

The Dutch DPA has published a [guideline](#) stating that web scraping by private parties and individuals is almost always illegal, as it typically involves collecting personal data, leading to GDPR violations. The DPA emphasizes that public information online does not equal consent for scraping. Exceptions are limited, such as household use or targeted scraping for specific business needs, but these must meet strict legal criteria. (May 2024)

## €290 million fine for global ride-hailing company

The Dutch DPA has imposed a fine of €290 million on a global ride-hailing company. The DPA found that the company transferred personal data of European taxi drivers to the United States without providing adequate measures to protect their personal data. According to the DPA, this constitutes a serious violation of the GDPR. The company has ceased the violation; it now uses the successor to the Privacy Shield to transfer the personal data to the United States. (July 2024)

## Dutch DPA's interpretation of legitimate interests is too strict

The Court of Justice of the European Union (CJEU) clarifies in case C-621/22 that purely commercial interests may not be categorically excluded from qualifying as legitimate interests. This decision challenges the strict stance taken by the Dutch DPA in recent years, which has held that commercial interests cannot be a valid basis for processing personal data without consent. The judgement of the CJEU will now be used by the Amsterdam's appeal court for a definitive ruling. (October 2024)

## New class action lawsuit against global social media platform

The Data Privacy Stichting and the Consumers Association, filed a new class action lawsuit against a global social media platform, seeking compensation for Dutch users. The lawsuit stems from improper handling of personal data, including sharing it with third parties and transferring it to the US without sufficient protection. Despite earlier court rulings and fines, the platform has not yet compensated users, leading to this renewed legal action. (March 2024)

## Appeal filed against another global social media platform

Stichting Take Back Your Privacy and the Consumers Association, filed an appeal in their class action lawsuit against a global social media platform. It challenges a January 2024 ruling that limited compensation to children registered before November 2022 and denied collective compensation for non-material damages. The foundation argues that all users, including after 2022, should collectively be eligible for non-material damage compensation. (July 2024)

## Class action lawsuit against another global social media platform

Stichting Data Bescherming Nederland has filed a class action lawsuit against a global social media platform, claiming it violated the privacy of millions of Dutch users by collecting and sharing personal data without proper consent. The data was used for targeted ads and shared with third parties, some outside the EU. The foundation seeks compensation for both material and non-material damages. (September 2023)

# ? What are the most relevant **cybersecurity updates?**

## **Dutch Cybersecurity Act and Critical Entities Resilience Act under consultation, implementation expected in 2025**

The Dutch government recently concluded its internet consultation for the implementation of the NIS2 and CER Directives, aimed at transposing these regulations into national law through the Cybersecurity Act (Cbw) and the Critical Entities Resilience Act (Wwke). These legislative proposals will align with the EU directives, setting out obligations for risk management, incident reporting, and cybersecurity resilience across critical and essential sectors.

Sector-specific supervisory authorities will be designated to oversee compliance, ensuring that relevant expertise is applied according to each sector's needs. Additionally, a registration mechanism will be managed by the National Cyber Security Centre (NCSC), enabling regulated entities to register and manage their compliance data through a dedicated portal. Due to the complexity of these developments, the Ministry of Justice and Security expects the law to take effect between Q2 and Q3 of 2025, rather than the initially planned deadline of October 2024.

Market research in the Netherlands has revealed that many companies underestimate the consequences of a cyberattack, leaving many businesses unprepared for NIS2. As for personal liability for board members, the Dutch implementation law currently does not specify particular details. However, board members are required to meet the knowledge and skill standards within two years, this must be kept up to date and proven through certification.

## **NIS2 Quickscan launched by government**

The Dutch government launched the [NIS2 Quickscan](#), a tool designed to help organizations understand how to prepare for the upcoming European NIS2 Directive.

The NIS2 Quickscan is specifically designed for IT and cybersecurity specialists and managers within organizations. By answering 40 yes/no questions, they gain insight into their organization's current digital resilience status. The Quickscan also provides actionable guidance, offering technical and organizational measures for each theme that can enhance digital resilience and help organizations prepare for NIS2 compliance.



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

## **Third Algorithmic Risks Report published**

The Dutch DPA has issued its third [Algorithmic Risks Report](#), emphasizing that while AI is rapidly evolving, its risk management is lagging. The DPA warns that the use of AI in the Netherlands must be approached with caution, as the country should prepare for an increase in AI-related incidents. The report highlights that public trust in AI is low, with concerns around misuse, privacy violations, and discrimination becoming more prevalent. The DPA calls for organizations to thoroughly understand the risks of AI before implementation, recommending measures such as random sampling to reduce discrimination.

Additionally, it highlights the limited awareness municipal organizations have of AI systems used by public entities, noting that representatives often lack sufficient knowledge, which hinders effective democratic control. Lastly, the DPA urges the government to strengthen the national AI strategy, ensuring stricter algorithm registration, especially in semi-public sectors like education and healthcare.

## **Dutch Authority for the Financial Markets and the Dutch Bank publish report on the impact of AI**

The Netherlands Authority for the Financial Markets and the Dutch Bank published the report "The impact of AI on the financial sector and supervision" with starting points and points of attention for shaping the supervision of artificial intelligence in April 2024. Both authorities would like to enter into a dialogue with the sector.

## **Supervisory authorities call for coordinated AI oversight**

The Dutch DPA and the Dutch Authority for Digital Infrastructure have urged the government to prioritize collaboration among regulators for AI oversight as the first set of rules of the EU AI regulation are set to take effect in early 2025. They stress the need for clear roles and sufficient resources to ensure timely guidance and enforcement. Both authorities propose aligning AI oversight with existing sectoral frameworks, designating the Dutch DPA as the primary authority for market compliance. They propose two exceptions to this principle: AI in the financial sector would remain under the supervision of the Dutch Authority for the Financial Markets and the Dutch Bank, while critical infrastructure oversight would be managed by the Dutch Authority for Digital Infrastructure and Human Environment and Transport Inspectorate (ILT).

## **Dutch DPA warns of data breach risks with AI chatbots**

The Dutch DPA has recently received multiple reports of data breaches involving employees entering sensitive personal information, such as medical records and customer addresses, into AI chatbots. This can result in unauthorized access by chatbot providers, which constitutes a serious privacy violation. The DPA emphasizes the need for organizations to set clear policies on chatbot use and to specify which data can and cannot be shared. It also suggests that companies could arrange with their chatbot provider that it won't store the data.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## **Data Protection Collective Act still under review in parliament**

The Data Protection Collective Act (Verzamelwet gegevensbescherming) was proposed to update and align privacy laws with ongoing digital developments. This legislative amendment focuses on revising the Dutch GDPR Implementation Act (UAVG) and other relevant regulations to provide new guidelines for various professional groups, such as curators, administrators, and accountants, regarding the processing of personal data. It also includes specific rules for financial institutions concerning transaction monitoring.

Although the proposal was submitted in 2022, it is still under deliberation in the House of Representatives (Tweede Kamer). The expected changes will only take effect once the act is approved, but the timeline for this remains unclear.

## **Data sharing act (WGS) approved by senate, set for 2025**

The Data Processing by Partnerships Act (Wet gegevensverwerking door samenwerkingsverbanden) is set to come into force on 1 January 2025, following approval by the Dutch Senate (Eerste Kamer). The act establishes a legal framework for sharing personal data among public and private entities to combat crime and fraud, introducing criteria for information sharing, mandatory privacy audits, and specialized training. Despite approval, it remains controversial due to privacy concerns, with critics comparing it to the previously banned SyRI system. The Council of State (RvS) has recommended further adjustments, including independent advisory committees and clear policies on data retention.

# Türkiye

## Contacts



**Lerzan Nalbantoğlu**

Partner, DL Attorneys at Law, Deloitte Turkey  
[lnalbantoglu@dlhukuk.com](mailto:lnalbantoglu@dlhukuk.com)



**Hande Çağla Yılmaz**

Associate, DL Attorneys at Law, Deloitte Turkey  
[handeyilmaz@dlhukuk.com](mailto:handeyilmaz@dlhukuk.com)

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

## **Amendments to the processing of special categories of personal data**

With the enactment of the Law on the Amendment of the Code of Criminal Procedure and Certain Laws and the Statutory Decree Law with No. 659, which was published in the Official Gazette on 12 March 2024, amendments to the Turkish Personal Data Protection Law (PDPL) entered into force as of 1 June 2024. These changes are to ensure the amended articles of the PDPL are compatible with the EU General Data Protection Regulation (GDPR).

The systematics of processing special categories of personal data has been changed by amending Article 6, paragraph 2 of the PDPL. In other words, from now on, it will be possible to talk about the exceptional cases in which special categories of personal data can be processed, rather than the conditions for processing them.

For example, prior to this change, employers had to obtain explicit consent from employees in order to fulfill their obligations to ensure occupational health and safety arising from the labor law. In line with the changes, employers can now process their employees' health data without obtaining the employees' explicit consent if necessary.

## **Amendments to the transfer of personal data abroad**

Article 9 of the PDPL before the amendments followed the systematic of “safe country list - undertaking - explicit consent”. However, after the amendments the systematic of “adequacy decision - appropriate safeguards – derogations for specific situations” was adopted.

The adequacy decision will be re-evaluated by the Personal Data Protection Board within every four years. However, to date, no adequacy decision has been taken by the board on either a country or sectoral basis.

In the event when the adequacy decision is absent, the companies may rely on appropriate safeguards, which are: binding corporate rules (BCR), standard contracts (SSC), undertaking, agreements between public institutions and organizations that are not international agreements.

The derogations for specific situations means the transfer of personal data abroad in some exceptional cases where there is no adequacy decision and one of the appropriate safeguards stipulated in the fourth paragraph of Article 9 of the PDPL cannot be provided. In other words, derogations for specific situations are personal data transfers, which are on a one-time or several-time basis and without continuity.

## Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad

Upon the amendments made within the scope of the PDPL regarding the transfer of personal data abroad, the relevant regulation was published on 10 July 2024. In particular, the regulation provides a detailed framework on what needs to be done upon an adequacy decision, appropriate safeguards and derogations for specific situations.

Within the scope of the amendments and the regulation, obligations have been foreseen for the first time in terms of the data processor. Before the amendments, the data processor was only a legal actor of the Turkish personal data protection law, but after the amendments, the PDPL has been more aligned with the GDPR, and some responsibilities have been foreseen also in terms of the data processor.

In addition, the regulation includes detailed regulations regarding standard contracts and information on standard contract preparation and signature processes.

## Privacy in the Digital Age: Protection of Children's Personal Data

The authority's fifth bulletin titled "Privacy in the Digital Age: Protection of Children's Personal Data" was published on the authority's official website. The following issues were mentioned regarding the processing of children's personal data in the bulletin:

- Parental sharing of children on social media (sharenting)
- Safer play for children in five steps:
  - Checking the age limit to find out which age group it is suitable for;
  - Finding out if the game has parental controls;
  - Checking if children can communicate with strangers via in-game methods;
  - Paying attention to whether the games have camera, sound, chat room, online communication features and if so, which age groups they are open to;
  - Checking the game's privacy settings; and
  - Reviewing the game's disclosure text.



# ? What are the most relevant **cybersecurity updates**?

## **The National Cyber Security Strategy and Action Plan 2024-2028**

The Ministry of Transport and Infrastructure published the National Cyber Security Strategy and Action Plan (2024-2028) with the aim of protecting the assets of institutions, organizations and users due to the fact that both private and public institutions and organizations carry out a significant part of their business volume in cyber environments and individuals frequently use these environments in their daily life, business and relationships.

The strategy and action plan was prepared based on four components, namely human, defense, deterrence and cooperation. Six main objectives were identified:

- Cyber resilience;
- Proactive defense and deterrence;
- A human-centered approach to cybersecurity;
- Safe use of technology and its contribution to cybersecurity;
- Domestic and national technologies in the fight against cyberthreats; and
- Türkiye's brand in the international arena.

## **Regulation based updates in Türkiye related to cybersecurity**

Although Türkiye does not have a regulation that is specifically for cybersecurity, there are regulations explicitly applicable to some sectors. For instance, the energy sector is among the sectors that are regulated in terms of cybersecurity. On 20 February 2001, Regulation on Cybersecurity Competency Model in Energy Sector had entered into force and there has since been amendments on 28 January 2024.

The scope of Regulation on Cybersecurity Competency Model in Energy Sector is to continuously improve the cybersecurity of industrial control systems used in the energy sector according to evolving needs and threats, to define the minimum acceptable level of security and to regulate the procedures and principles regarding the cyber resilience, adequacy and maturity of these control systems.

Following the recent amendments, three new classes have been added to the control items that liable organizations are obliged to perform by Regulation on Cybersecurity Competency Model in Energy Sector: natural gas storage, natural gas and raw material petroleum transmission, and electricity transmission organizations are also obliged to perform controls.



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

## Ethical guidelines on the use of GenAI

In the guide published by the Council of Higher Education on its website on 7 May 2024, ethical values in the use of Generative AI were examined. The values in question were expressed as transparency, integrity, lawfulness, duty of care, fairness and protection of confidentiality and privacy, accountability and responsibility, and contributing to the ethical prospect. In terms of data ethics, it was emphasized in the guideline that the following issues should be taken into consideration:

- Data source and permission to use the data;
- Data confidentiality and privacy;
- Data bias;
- Generative AI hallucinations;
- Data currency;
- Data reliability; and
- Intellectual property rights.

## National Cyber Security Strategy and Action Plan (2024-2028)

The Ministry of Transport and Infrastructure has published the National Cyber Security Strategy and Action Plan (2024-2028) with the aim of protecting the assets of institutions, organizations and users.

The published strategy and action plan has been prepared based on four components, which are human, defense, deterrence and cooperation. In addition, six main objectives have been determined:

- Cyber resilience;
- Proactive defense and deterrence;
- Human-centered cybersecurity approach;
- Safe use of technology and its contribution to cybersecurity;
- Domestic and national technologies in combating cyberthreats; and
- Türkiye's brand in the international arena.

## Bill proposal on artificial intelligence

The bill regarding artificial intelligence was submitted to the Grand National Assembly of Türkiye on 25 June 2024. In the rationalization of the bill, it is stated that AI technologies are rapidly developing, becoming widespread in many areas of life, bringing about revolutionary changes in critical areas such as health, education, security and transportation, but these developments have led to an increase in the malicious use of AI technologies and threaten the rights and freedoms of individuals, therefore it is aimed to determine the legal framework and to ensure that artificial intelligence technology is developed and used in a fair and ethical framework. The bill is still under review in the commission. Steps are expected to be taken in the future.

## Digital Transformation Support Program

In the Official Gazette dated 26 July 2024 and numbered 32613, the Communiqué on the Implementation Principles of the Digital Transformation Support Program was published and entered into force. Within the scope of this communiqué, artificial intelligence is also included in the scope of digital transformation. The purpose of the communiqué is to implement the published strategy and development plans within the framework of the digital transformation support program. The communiqué regulates the minimum qualifications to be provided by the organizations wishing to receive support under the digital transformation program and the decision process as a result of the examinations to be carried out by the General Directorate of National Technology of the Ministry of Industry and Technology.



# What are the most relevant expected developments in **data protection**?

## **Amendments on Personal Data Protection Law regarding GDPR**

As of 1 June 2024, the provisions of the PDPL regarding special categories of personal data and the transfer of personal data abroad have been amended, bringing them closer to the GDPR. Accordingly, it is expected that other articles of the PDPL will be amended in the future to bring them closer to the GDPR.

## **A Guide on Amendments on Personal Data Protection Law**

It is expected that a guide will be published regarding the transfer of personal data abroad. It is expected that the question marks in the application following the latest PDPL changes will be resolved with the publication of this guide.

## **A module regarding standard contracts' notification to the authority**

With the 1 June 2024 amendment to the law, standard contracts have been determined as one of the appropriate security methods for transferring personal data abroad. The authority has published four different types of standard contracts on its official website and has foreseen that the signed standard contracts will be reported to the authority. It is anticipated that a module will be published in the future and standard contracts will be notified to the authority through this module.



# Ukraine

## Contacts



**Dmytro Pavlenko**

Partner, Deloitte Legal Ukraine

[dpavlenko@deloittece.com](mailto:dpavlenko@deloittece.com)



**Anton Bychkov**

Senior Managing Associate, Deloitte Legal Ukraine

[anbychkov@deloittece.com](mailto:anbychkov@deloittece.com)

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

## Overview of current national data privacy laws in Ukraine

The basis for personal data protection is the Law of Ukraine “On Personal Data Protection” (the Law). This regulatory act was prepared based on Directive 95/46/EC “On the Protection of Individuals with Regard to Processing Personal Data and Free Movement of Such Data”. The provisions of the Law define the requirements to processing personal data, rights of personal data subjects, and grounds for their processing.

At the same time, it should be emphasized that, since the Law was developed based on the previous Directive 95/46/EC and adopted more than 10 years ago, it does not sufficiently address the current challenges of personal data protection.

Another important bylaw is the Model Procedure for Personal Data Processing, as approved by Order of the Ukrainian Parliament Commissioner for Human Rights No. 1/02-14 dated 8 January 2014. However, this is an explanation; in practice, during its inspections, the regulator oversees the compliance with its provisions. It addresses the requirements for personal data processing.

It is important to note that, by signing the Association Agreement between the European Union and Ukraine, Ukraine has committed itself to meeting high data protection standards. In this context, in 2022, the Draft Law on Personal Data Protection No. 8153 was submitted to the Verkhovna Rada which aimed to harmonize the Ukrainian legislation with General Data Protection Regulation (GDPR). This draft Law is currently under consideration, but its adoption will be a significant step toward strengthening personal data protection in Ukraine.

## Restrictions on the right to privacy under the martial law

The legal regime of the martial law was introduced in Ukraine on 24 February 2022.

According to the Decree of the President of Ukraine No. 64/2022 dated 24 February 2022, some constitutional rights and freedoms of persons, including the right to non-interference in their private and family life, may be temporarily restricted during the period of the martial law.

Considering the martial law regime and full-scale Russian invasion, the Ukrainian Parliament Commissioner for Human Rights has developed some recommendations:

- On the protection of personal data in the conditions of the martial law; and
- On some issues of personal data processing during the provision of humanitarian and charitable assistance.

# ? What are the most relevant **cybersecurity updates**?

## Cybersecurity in Ukraine in the context of the NIS2 Directive

Although Ukraine is not a member of the EU and, therefore, the NIS2 Directive is not a part of Ukrainian laws, the Ukrainian authorities are aware of its provisions and requirements.

In November 2023, the State Service for Special Communications and Information Protection of Ukraine (the SSSCIP, regulator in the area of cybersecurity) and the National Coordination Center for Cyber Security (the NCCC) under the National Security and Defense Council of Ukraine concluded a Working Agreement with the European Union Agency for Cyber Security (the ENISA). The agreement covers short-term structured cooperation actions, including implementation of the key acts such as NIS2 and acts in such sectors as telecommunications and energy.

## Recent cybersecurity regulatory updates

Some recent regulatory updates:

- Order of the SSSCIP's Administration No. 1011 dated 1 December 2023 "On Approval of Recommendations for the Development of a Critical Infrastructure Protection Plan for the National Level Project Threat of "Cyber Attack/Cyber Incident"".
  - These recommendations include tips on preparing for cyber threats, algorithms for dealing with cyber attacks, and requirements for information protection based on the Ukrainian laws and regulations. The guidelines provide instructions on how to create a protection plan, including: identifying persons responsible for cyber protection, describing the overall functional scheme of the system, monitoring and responding to cyber incidents, training personnel, using encryption and other security measures for all stages of preparation, response, and recovery of systems after incidents.

- Resolution of the Cabinet of Ministers of Ukraine No. 415 dated 28 April 2023 "On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Objects, Inclusion of Such Objects in the Register, Access and Provision of Information from it".
  - This resolution establishes the procedures for forming and maintaining the Register of Critical Infrastructure Objects, including critical infrastructure objects in the register, details of the register functioning. This register is operational, but the information contained in it is not publicly available.
- Resolution of the Cabinet of Ministers of Ukraine No. 299 dated 4 April 2023 "Certain Issues of Responding by Cybersecurity Entities to Various Types of Events in Cyberspace".
  - This resolution defines the procedures for responding to various types of events in cyberspace and categories (levels) of their criticality.

## Military-related regulatory updates

Also, since there is the regime of the martial law in Ukraine and full-scale invasion, military related cyber regulations are constantly developing.

On 18 June 2024, the Cabinet of Ministers of Ukraine adopted Resolution No. 719 "Certain Issues of Protection of State Information Resources and Restricted Information Used by the Ministry of Defense and the Armed Forces". In practice, it allows to use cyber defense software and hardware developed and approved by the NATO partner countries without a need for additional certification in Ukraine. This may accelerate and simplify the process of implementing modern cybersecurity solutions.





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

## Overview of general approach on development of AI regulation in Ukraine

The Ukrainian regulation on AI matters is currently in the development stage.

The Ministry of Digital Transformation of Ukraine presented in June 2024 the White Paper on Artificial Intelligence Regulation in Ukraine.

The Ministry of Digital Transformation of Ukraine adopts a flexible, business-friendly approach to AI regulation, aiming to balance innovation with human rights protection. The ministry emphasizes a gradual regulatory framework, starting with non-binding tools, such as regulatory sandboxes, voluntary codes of conduct, and risk assessments. This allows businesses to prepare for future mandatory regulations, which will be harmonized with the EU's AI Act. The ministry seeks to foster AI innovation while ensuring alignment with the EU integration, with special exemptions for the defense sector to maintain national security.

Their approach is designed to maintain Ukraine's competitiveness in the AI market, encouraging responsible AI development while adapting to global and the EU standards. They focus on supporting small and medium businesses and startups, providing them time and tools to comply with regulations before legally binding measures are enacted. This incremental approach reflects the government's belief that Ukraine needs time to develop regulatory capacity, drawing on international best practices to shape an effective AI governance framework.

### White Paper on AI Regulation is based on a two-stage roadmap

- Stage 1 (2024-2026): Preparatory phase involving non-legislative tools such as regulatory sandboxes, voluntary AI system labeling, AI risk assessments, and codes of conduct. The goal is to give businesses time to adapt and align with future regulations.

### Tools:

- Regulatory sandbox for AI products;
- AI labeling system;
- AI impact assessment methodology; and
- Legal advisory platform for AI compliance.

These tools are designed to assist businesses in preparing for the future regulatory environment while maintaining competitiveness and human rights protection.

- Stage 2 (2026-2027): Introduction of mandatory AI regulation. This stage involves the adoption of the legislation similar to the EU's AI Act. The Ukrainian government will develop a law in line with the EU AI Regulation to ensure compliance with international standards and to protect human rights while fostering innovation.

The adoption will be gradual with the possibility of deferring the enforcement of certain provisions, giving businesses time to comply. The creation of a regulatory authority is expected at this stage to oversee the implementation of the law and monitor compliance.

### Key elements:

- Phased implementation of the EU-style regulations;
- Establishment of a regulatory body to enforce the AI law; and
- Continued harmonization with the European Union standards as part of Ukraine's integration efforts.





# What are the most relevant expected developments in data protection, cybersecurity and AI?

## Trends and prospects in the personal data protection legislation

### The Draft Law of Ukraine “On Personal Data Protection” No. 8153

In October 2022, the Verkhovna Rada of Ukraine registered the Draft Law of Ukraine “On Personal Data Protection” No. 8153 (the Draft Law 8153), which proposes significant changes in the area of personal data protection in Ukraine.

The following key innovations of the Draft Law 8153 are envisaged:

- A range of rights of personal data subjects has been expanded, in particular, the right to be forgotten, data mobility, and restriction on processing. The conditions for obtaining consent to data processing are also spelled out in more detail, which is in line with the principles of transparency and accountability;
- International data transfer is regulated in more detail; and
- A significantly increased liability for violation of the rules of personal data processing and protection. The amount of fines, depending on the offense, can range from approximately €230 to €444,000 for individuals, and from €670 to €3.33 million or from 0.05-0.1% to 8% of the total annual turnover for legal entities. As of now, such a fine is approximately from €40 to €750.

### The Draft Law of Ukraine “On the National Commission for Personal Data Protection and Access to Public Information” No. 6177

Another relevant act is the Draft Law of Ukraine “On the National Commission for Personal Data Protection and Access to Public Information” No. 6177 (the Draft Law 6177), which provides for the establishment and operation of a new supervisory authority in the information sphere –

the National Commission for Personal Data Protection and Access to Public Information. One of the main tasks of the commission is to ensure that controllers and personal data operators comply with the Law on Personal Data Protection.

To summarize, trends in the Ukrainian legislation demonstrate an intention towards a stricter protection of personal rights and increased responsibility of organizations working with personal data. The new draft laws are based on European standards but retain the specifics of the Ukrainian jurisdiction. There is hope that the adoption of these acts will bring to recognizing Ukraine by the EU as a country with adequate data protection.

## Calendar plan for development of AI regulation

**2024–2026:** Focus on preparatory non-legislative tools, industry adaptation, and capacity building for both businesses and the state.

**2026-2027:** Development and implementation of the national AI legislation following the adoption of the EU AI Regulation, with progressive enforcement of different legal provisions.

This approach emphasizes flexibility and international integration while considering the importance of innovation, human rights, and Ukraine’s goal of joining the European Union.

## Cybersecurity strategy

The Cabinet of Ministers of Ukraine issued Resolution No. 1163-r dated 19 December 2023 “On Approval of the Action Plan for 2023-2024 to Implement the Cybersecurity Strategy of Ukraine”.

In particular, the following activities are planned for Q4 2024:

- Create a nationwide system for detecting cyberattacks, counteracting acts of cyberterrorism and cyberespionage against critical information infrastructure;
- Implement a centralized system of cyber defense of information resources of foreign diplomatic missions of Ukraine and state properties of Ukraine abroad;
- Create a joint platform with international partners to exchange information on destructive activities in cyberspace;
- Develop and approve basic requirements and recommendations on cybersecurity for cybersecurity entities; and
- Ensure the development of a network of cyberattack and cyber incident response centers.

## Other potential updates of cybersecurity legislation

The Draft Law No. 11290 dated 27 May 2024 intends to establish rules for companies that supply goods and services for government computer systems. Suppliers may have to comply with security requirements according to the risk level of their products.

# United Kingdom

## Contacts



**Cavan Fabris**

Partner, Deloitte Legal United Kingdom

[cfabris@deloitte.co.uk](mailto:cfabris@deloitte.co.uk)



**Katherine Eyres**

Director, Deloitte Legal United Kingdom

[keyres@deloitte.co.uk](mailto:keyres@deloitte.co.uk)

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

## Data (Use and Access) Bill

On 23 October 2024, the UK government published the highly anticipated [Data \(Use and Access\) Bill](#) (Data Bill), which introduces reforms across wide-ranging areas spanning digital identity to data protection. At a high level, key features of the new Data Bill include:

- Online safety provisions, including a new data preservation process for online safety purposes, particularly in relation to child death investigations – this supports the ongoing implementation of the UK's Online Safety Act by Ofcom, the UK's online safety regulator.
  - A framework to set up smart data schemes, which:
    - Will empower businesses and consumers to share their data with regulated and authorized third parties;
    - Include key provisions covering regulatory powers for issuing data sharing protocols, the creation of interface bodies, and also open finance expansion; and
    - According to government [guidance](#), will aim to deliver benefits for consumers, such as enabling price comparison between energy providers to secure better deals and authorizing third party data intermediaries, thereby making the process for consumers to switch service providers easier.
  - Establishment of a Digital Verification Services (DVS) trust framework, outlining rules for DVS providers, including “trust marks” and a register of certified digital identities providers, and clarity regarding the legal status of digital identities.
- Targeted reforms to the existing UK data protection regulatory regime, including to:
    - Support the use of data in beneficial AI and data-driven innovation;
    - Provide clarity regarding processing for research purposes (in particular, an expanded definition of ‘scientific research’ that captures some privately funded commercial research);
    - Introduce a new lawful basis for processing personal data based on “recognized legitimate interest”, encompassing situations such as safeguarding vulnerable individuals, crime prevention, emergency response, and national security;
    - Relax certain limitations on solely automated decisions with legal or similarly significant effects on individuals, and shifting focus towards restricting automated decision-making when using special categories of personal data;
    - Introduce proportionality measures related to data subjects' rights, including clarifying time limits for data subject rights requests and defining “reasonable and proportionate” searches for personal data in response to such requests;
    - Refine the “purpose limitation principle” to expand when personal data collected for one purpose can be used for a different but “compatible” purpose;
    - Introduce a more flexible “data protection test” for assessing the adequacy of data protection in other countries in the context of international data transfers; and
    - Restructure the current UK data protection regulator, the Information Commissioner's Office (ICO), into an “Information Commission” with more robust governance structure and enhanced enforcement powers.





## Expected impacts of the reforms

The government [estimates](#) that the Data Bill will boost the UK economy by £10 billion across 10 years by using the power of data to accelerate investment and innovation.

The proposed reforms will however increase divergence from the European Union General Data Protection Regulation (EU GDPR) – in some areas, this may give greater clarity or in fact raise the bar in terms of data protection compliance, but in other areas, the regulatory compliance burden on organizations may be lessened.

This is important in the context of the upcoming renewal of the current European Commission's (EC) data adequacy decision for the UK, which is set to expire on 27 June 2025. As part of the renewal process, the EC will assess the new law's impact on UK data protection standards to determine if the same level of protection for personal data is maintained in the UK as under the EU GDPR.

## What next?

The Data Bill will now begin its legislative journey in the House of Lords before going to the House of Commons. It is expected to receive Royal Assent and become law in early to mid 2025.

## Biometric data

On 5 March 2024, the ICO published its [guidance](#) on how data protection law applies when using biometric data in biometric recognition systems following consultation with stakeholders in 2023. It outlines the law and recommendations for good practice in this area.

The guidance notes that biometric recognition systems are used to uniquely identify people, and that 'biometric recognition' therefore encompasses all situations in which biometric data is special category data. It further notes that explicit consent is likely to be the most appropriate processing condition, except in instances where consent is not possible, such as in the case of systematic monitoring of public spaces. However, when relying on consent, suitable alternatives e.g., use of a PIN or password must be offered.

In order to remain compliant with data protection law when using biometric data, the guidance states that:

- A data protection by design approach must be taken when putting in place biometric recognition systems;
- A DPIA must be completed before using a biometric recognition system;
- The impact of a biometric recognition system on data subjects must be assessed;
- It must be made clear who is the controller of the biometric data; and
- A written contract must be put in place with all processors.

Biometric data is one of the ICO's three key areas of focus for 2024/25. The guidance comes in the wake of [enforcement action](#) taken against Serco Leisure in February 2024 related to their processing of facial recognition technology and fingerprint scanning to monitor the attendance of 2,000 leisure center employees.

## Children's privacy

The ICO has identified children's privacy as another of its three key priority areas for 2024/25, along with biometric data and ad tech.

On 3 April 2024, the ICO published its [2024/25 priorities](#) for protecting children's personal information online through a new Children's Code Strategy, which will focus on:

- **Default privacy and geolocation settings:** Children's profiles must be private and geolocation services turned off by default;
- **Profiling children for targeted advertisements:** Profiling should be off by default unless there is a compelling reason to use it for targeted advertising;
- **Using children's information in recommender systems:** Mitigating the impacts of harmful content feeds generated by algorithms using behavioral profiles and children's search results; and
- **Using information of children under 13:** Parental consent will be required as children under the age of 13 cannot give consent to their personal information being used by an online service

The ICO has confirmed that it will be working closely with other UK regulators such as Ofcom, as well as international regulators, to raise global data protection standards in relation to children's privacy.

It also published an updated [Commissioner's Opinion on age assurance](#) on 18 January 2024.

## Ad tech

After announcing in 2023 that it was planning on assessing the cookie compliance of the UK's 100 top websites, the ICO issued a [statement](#) on 31 January 2024 confirming that it had written to 53 of these websites warning of enforcement action if they failed to make the appropriate changes to their advertising cookies, and that it received an 'overwhelmingly positive response'.

The ICO later confirmed in a [statement](#) on 17 September 2024 that 52 of the 53 websites contacted have engaged, making the appropriate changes to how advertising cookies are used. However, ad tech remains a key area of focus for the ICO in 2024/25. In this same statement, the ICO confirmed that it has issued a reprimand for processing data through advertising cookies without consent, by sharing personal data with advertising technology companies as soon as people accessed the SkyBet website and before they had an option to accept or reject advertising cookies.

The ICO has reaffirmed its commitment to cracking down on non-compliant ad tech and has also announced that it has audited a number of data management platforms to further understand how the wider industry handles personal data, some of which are now under investigation for potential infringements.

Updated guidance on the use of cookies and tracking technologies is expected by the end of 2024, following a consultation on 'consent or pay' business models which closed on 17 April 2024.

# ? What are the most relevant **cybersecurity updates?**

## **New Cyber Security and Resilience Bill**

As part of the July 2024 King's Speech, the [Cyber Security and Resilience Bill](#) (Cyber Bill) was proposed in response to the increasing frequency and severity of cyberattacks affecting entities in critical sections and their supply chains.

The Cyber Bill aims to address existing vulnerabilities and strengthen the UK's defense against cyberthreats by expanding the scope of the current cyber regulations, empowering regulators and increasing reporting requirements.

The recent draft implementing regulation, which will apply to entities such as cloud computing service providers, data center providers, providers of online marketplaces, search engines and social network platforms, sets out technical and methodological requirements for risk management measures and the criteria for when an incident can be considered significant for those entities.

The Cyber Bill will provide updates to expand the remit to offer better protection to supply chains and digital services more widely. Furthermore, it will allow regulators to take a stronger stance on enforcing cyber safety measures and ensure the framework is being implemented.

Further detail has recently been released on the proposed reclassification of data centers as so-called critical national infrastructure, meaning data centers will need to comply with higher security standards and be subject to more stringent government oversight.

This is alongside increased investment in data center infrastructure. Benefits for consumers should mean NHS, financial and personal smartphone data will be safer from cyberattacks, environmental disasters and IT blackouts.

There may also be wider resulting effects for all businesses when evaluating third-party and internal hosting locations if the UK establishes itself as a leader in secure and stable data centers.

## **UK PSTIA Regulations come into force**

On 29 April 2024, the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (PSTIA Regulations) came into force.

The [PSTIA Regulations](#) are intended to enforce consumer protections against hacking and cyberattacks by mandating that internet-connected smart devices meet minimum security standards. In particular, the PSTIA Regulations set out the following:

- **Passwords:** Each product requires a unique password, or product users must be capable of defining the password. This, for example, includes a requirement that passwords must not be derived from publicly available information or be easily guessable.
- **Reporting security issues:** Manufacturers must provide free, accessible, clear and transparent information on how product security issues should be reported to them, timescales on acknowledgment of receipt, and status updates until resolution.
- **Minimum security update periods:** Information on minimum security update periods, including the minimum length of time and an end date, must be published and made available to consumers.

The PSTIA Regulations will be enforced by the Office for Product Safety and Standards, the existing enforcer of UK product safety regulations.



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

## UK government publishes initial guidance for regulators on implementing the UK's AI regulatory principles

In February 2024, the Department for Science, Innovation & Technology (DSIT) published [guidance](#) for regulators to support them in developing tools and guidance to implement the UK's approach to AI regulation, building upon the AI Regulation White Paper (the white paper) published in 2023. This represents phase one of DSIT's intended three-phase guidance approach. The previous Conservative government was due to release its phase two guidance in summer 2024, which was intended to expand on the initial guidance and provide further detail informed by feedback from regulators and other stakeholders, but this is yet to arrive and (as at the date of writing) its status remains uncertain.

## UK ICO publishes strategic approach to regulating AI

On 30 April 2024, the ICO published its [strategic approach](#) to regulating AI in response to a request by the Secretary of State for Science, Innovation and Technology.

Although the ICO did not consider that new legislation would be required to regulate the risks posed by AI, it welcomed the government's approach to strengthening existing regulators and ensuring that they are appropriately resourced in order to allow them to hold organizations to account. This comes following the DSIT's announcement in its white paper consultation response of a £10 million package to boost regulators' AI capabilities.

The ICO noted that the principles set out in the white paper mirror the principles of data protection law, which the ICO already oversees, and that it therefore already has experience in implementing the objectives set out in the white paper.

## UK and US sign Memorandum of Understanding on AI safety

In November 2023, the UK and US governments announced the establishment of their respective AI Safety Institutes with the aim to work together towards the safe development of AI.

On 1 April 2024, a [Memorandum of Understanding](#) (MoU) was agreed by the two governments, which re-states their aim for the Institutes to work closely to achieve their shared objectives on AI safety. The MoU specifically outlines the Institutes' plan to:

- Develop a common approach on model evaluations;
- Perform at least one joint testing exercise on a publicly accessible model;
- Collaborate on AI safety technical research;
- Explore personnel exchanges;
- Share information across the breadth of their activities;
- Develop similar collaborations with other countries to promote AI safety and manage frontier AI risks; and
- Work with other governments on international standards for AI safety testing.



## AI regulation in state of flux with change of UK government

Following the UK general election on 7 July 2024, there was change of UK government to the Labour Party, which is still formulating its proposals for AI regulation.

The previous [Artificial Intelligence \(Regulation\) Private Members' Bill](#) (PMB), which was introduced to the House of Lords in November 2023, sought to establish a central AI authority to oversee the UK's regulatory approach to AI and introduce various principles and safeguards related to responsible AI use. However, as the PMB was not enacted prior to the prorogation of parliament, it failed.

As yet, the new UK government has not committed to introducing AI-specific legislation, but the government has indicated that its priority is to specifically regulate the developers of the most powerful AI models.

The UK at present has an AI regulation framework that draws on existing laws and regulations (including the Data Protection Act 2018 (incorporating the UK GDPR)).

In contrast, the EU has enacted specific legislation by way of the EU AI Act, which establishes a regulatory legal framework for the use of AI models and systems within the EU.

## New Regulatory Innovation Office (RIO) launched

On 8 October 2024, the UK government launched the RIO to speed up public access to new technologies. According to the [press release](#), this inter-sectoral and cross-government initiative is intended to support “regulators to update regulation, speeding up approvals, and ensuring different regulatory bodies work together smoothly. It will work to continuously inform the

*government of regulatory barriers to innovation, set priorities for regulators which align with the government's broader ambitions and support regulators to develop the capability they need to meet them and grow the economy”.*

The RIO will initially focus on those areas of engineering biology, space, AI and digital and healthcare and connected and autonomous technology that have the power to change people's lives for the better.

## UK ICO launches consultation on Generative AI and data protection

The ICO launched a [consultation series](#) closing on 18 September 2024 with an aim to provide further clarity on how data protection law should apply to the use of Generative AI (GenAI). The consultation series covered the following ‘chapters’:

- The lawful basis for web scraping to train GenAI models;
- Purpose limitation in the GenAI lifecycle;
- Accuracy of training data and model outputs;
- Engineering individual rights into GenAI models; and
- Allocating controllership across the GenAI supply chain.

The input received during the consultation will be used to update the ICO's guidance on AI. The ICO is currently finalizing its review and is due to publish its findings before the end of 2024.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## EU-UK adequacy decision

The EU approved adequacy decisions for the EU GDPR (retained in UK law post-Brexit as the UK GDPR) and the Law Enforcement Directive on 28 June 2021, meaning data can, in most cases, continue to flow freely from the EU to the UK as it did before Brexit.

Both decisions are due to expire on 27 June 2025, and a review will be underway next year to determine whether the UK retains adequacy.

## Updated guidance – AI and data protection

In its [strategic approach](#), the ICO stated its intention to consult on updates to its [Guidance on AI and Data Protection](#) and [Automated Decision-Making and Profiling](#) in spring 2025, in order to reflect changes to data protection law envisaged by the previous Data Protection and Digital Information Bill. It remains to be seen whether these consultations will go ahead in the wake of the new Data Bill.

## New legislation

The Department of Science, Innovation and Technology announced on 30 September 2024 that the Cyber Security and Resilience Bill (as outlined on slide 331) will be introduced to parliament in 2025.

The Data (Use and Access) Bill was introduced to the House of Lords on 23 October 2024 and is set to begin its passage through the UK legislative process (as outlined on slides 328 to 329). The Information Commissioner has [welcomed](#) the introduction of the bill, describing it as “*an important piece of legislation which will allow my office to continue to operate as a trusted, fair and independent regulator and provide certainty for all organisations as they innovate and promote the UK economy*”, but the ICO’s full response to the bill and parliamentary debate on its provisions is awaited. We also await further information as to how the government proposes to regulate the developers of the most powerful AI models (and any other aspects of AI development and use).

The government will need to walk a fine line to ensure that the UK’s reformed regime will not be seen to be too light a touch on data protection, such that it could put the European Commission’s EU-UK adequacy decision at risk.

# Uruguay

## Contacts



**Javier Domínguez**

Senior Manager, Deloitte Legal Uruguay

[javdominguez@deloitte.com](mailto:javdominguez@deloitte.com)

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

## **The European Commission ratified that Uruguay is an adequate country for data transfer**

### **First review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC**

The European Commission ratified, through a report published and adopted on 15 January 2024, the recognitions of all countries that had been declared adequate during the validity of Directive 95/46/EC, the predecessor of the General Data Protection Regulation, including Uruguay.

This confirmation reaffirms that Uruguay's data protection scheme, modernized with successive reforms over the years, continues to provide individuals with protection equivalent to that offered by the GDPR in the EU.

Moreover, thanks to this decision, companies or organizations transferring personal data from the EU to Uruguay, and those that decide to do so in the future, provided they have a legitimate cause, will not require additional authorizations or protections, allowing for secure international trade with fewer barriers.

Only 15 countries in the world have been granted "adequate" status, and only two of them are from Latin America, including Uruguay.

## **URCDP issues adequacy decision on entities under the EU-US DPF**

### **Resolution No 63/2023**

In Uruguay, as a rule, and except for legally provided exceptions, the transfer of personal data of any kind to countries or international organizations that do not provide adequate levels of protection is prohibited.

Before the Privacy Shield and after the EU-US Data Privacy Framework, entities that wanted to transfer data to a data processor in the United States without the consent of the data holder had to adopt certain contractual clauses that ensured the proper handling of said data. And this contract had to be reviewed and approved by the Uruguayan data protection authority (URCDP).

However, under the new Resolution No. 63/2023, entities operating under the EU-US DPF are now recognized as having an adequate level of data protection for cross-border data transfers. Entities responsible for data processing that intend to conduct international transfers to organizations covered by the Privacy Framework must provide the URCDP with a simple formal declaration. This declaration should be submitted either when registering the database or before the data transfer and must confirm that the importing organization has extended the Privacy Framework's safeguards to the data being transferred from Uruguay.





## URCDP publishes data protection guide for MSMEs

On 16 May 2024, the URCDP published a comprehensive guide on personal data protection specifically designed for micro, small, and medium-sized businesses (MSMEs). This guide is intended to help MSMEs navigate the complexities of data protection regulations.

The guide is a valuable resource for MSMEs, as it includes a wide array of tools and resources aimed at simplifying the management of data protection practices. Among the key features are clear and concise definitions of crucial personal data protection concepts, which lay the groundwork for understanding the broader regulatory landscape.

To facilitate the management of data protection practices, the guide includes a variety of tools and resources: free tools, clause models, virtual courses, among others. By offering these resources, the guide aims to make it easier for MSMEs to implement effective data protection measures and maintain compliance with legal requirements.

# ? What are the most relevant **cybersecurity updates**?

## **Law on the Prevention and Repression of Cybercrime**

On 14 August 2024, the Uruguayan parliament approved the Draft Law on the Prevention and Repression of Cybercrime, thus taking a significant step forward in the regulation of illegal activities in the digital environment.

The law regulates the breach of data, among other crimes, and punishes with six to 24 months imprisonment anyone who, through the use of any telematic means, accesses, seizes, uses, or modifies confidential data of third parties, recorded in digital media, or any other type of public or private file or record, without the authorization of its owner.

The approval of this regulation marks a significant advancement in the regulation, prevention, and combat of cybercrimes in Uruguay, aligning with international standards such as the Budapest Convention of 2001.



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

## **Artificial Intelligence Readiness Assessment Report**

In July 2024, UNESCO publish their Artificial Intelligence Readiness Assessment Report of Uruguay.

The report presents 18 recommendations, which include advancing regulations, consolidating the institutional capacity of Agency for Electronic Government (AGESIC) and related public sector institutions, together with deepening the understanding around the environmental impact of AI systems and monitoring and evaluation, as well as capacity building and training efforts.



# What are the most relevant expected developments in data protection, cybersecurity and AI?

## National Cybersecurity Strategy

The National Cybersecurity Strategy is framed within the 10th goal of the Uruguay Digital Agenda 2025, which aims to strengthen national cybersecurity to prevent and mitigate risks in cyberspace, ensuring the availability of critical information assets.

The development of the project was structured through a six-stage co-creation process. The last two stages are pending:

- Approval: submission of the final version to the certain authorities and the formal process for final approval by the Executive Branch.
- Presentation and communication: publication of the National Cybersecurity Strategy and initiation of the follow-up, monitoring and evaluation process.

Therefore, the process is planned to be completed by the end of 2024.

## National Artificial Intelligence Strategy

In 2024, a draft version of the National Artificial Intelligence Strategy 2024-2030 was released for public consultation.

The primary actions proposed for the regulatory framework of artificial intelligence are as follows:

- Identify and address existing regulatory gaps that hinder effective governance by promoting appropriate regulatory measures, which may include binding or non-binding regulations, co-regulatory, and self-regulatory instruments.
- Conduct an assessment to identify regulatory gaps related to intellectual property and civil liability in AI, and develop frameworks based on national consensus to address these challenges.
- Establish specific regulatory frameworks for various sectors, such as health, education, and insurance, through multi-stakeholder collaboration.
- In accordance with Article 75 of Law No. 20.212 dated 6 November 2023, support the institutionalization of regulatory experimentation initiatives. These initiatives will create opportunities to test innovative products, services, or business models, generating evidence to inform regulatory decisions and guide regulated entities on applicable regulations. Tools such as regulatory sandboxes and innovation hubs will be considered for this purpose.

The final document is expected to be released soon.



# Contributors

Albania	Ened Topi   Jona Rapi
Argentina	Eduardo Patricio Bonis   Matías Homero Corbo   José María Martín
Australia	Rachel Sciascia   Hanna Seal   Celeste Bennett   Ashleigh Weeks
Austria	Sascha Jung   Christian Kern
Belgium	Matthias Vierstraete   Julie Van Com   Michaël Dours
Bulgaria	Miglena Micheva   Irena Koleva   Kristian Nemtsov
Cameroon	Sandrine Soppo Priso   Jacques Didier Makong   Marie Christiane Ngo Nlend   Paul Raoul Nhanag
Chile	Ruby Soteras   Oliver Ortiz   Nicolás Lopez
Colombia	Jose Luis Jerez   Laura Nataly Forero   Andrés Felipe Roncancio   Lucía Tamayo   Andrés Felipe Salazar
Croatia	Zrinka Vrtarić   Klara Jambrešić
Cyprus	Gaston Hadianastassiou   Christina Hadjivassiliou   Chrystalla Karalouka   Vivian Antoniou
Czech Republic	Jaroslava Kračúnová   Tomáš Maux   Marek Plný   Edita Bolková   Ondřej Švub
Denmark	Jeanette Vallat   Simone Mai Petersen

Ecuador	Manuel Cartagena   Sara Arias   Mónica Ron
Finland	Jean-Tibor IsoMauno   Toni Oras
France	Hervé Gabadou   Morgane Bourmault   Laura Mallard   Tony Baudot   Farah Agrebi
Germany	Nikola A. F. Werry   Jan Rudolph   Dr. Till Contzen   Sarah Marie Hofmann
Ghana	Wisdom Kpano   Naa Adzorkor Adzei   Naa Ayeley Komey   Maxine Seshie
Greece	Arianna Sekeri   Maria-Alexandra Papoutsis
Guatemala	Estuardo Paganini   Manuel Lara
Hungary	Dániel Nagy   Flóra Szalai
Iceland	Haraldur Ingi Birgisson   Alma Tryggvadóttir
Indonesia	Cornel B. Juniarto   Stefanus Brian Audyanto   Hakim Anantaputra
Italy	Ida Palombella   Pietro Boccaccini   Alessandro Amoroso   Valentina Forin
Ivory Coast	Ursula Dutauziet   Audrey Allo-Ello
Japan	Tetsuya Okura   Makoto Tsuruoka   Yuki Kajitani

# Contributors

Kosovo	Ardian Rexha   Vjollca Hiseni	Singapore	Gretchen Su
Luxembourg	Thomas Held   Sophie Brisson   Crystal Gocyk	Slovenia	Ana Kastelec   Majda Karajković   Nika Logar
Mexico	Mauricio Oropeza   Melissa Franco	Spain	Rodrigo González Ruiz   Carlos de Jorge Pérez   Itxaso Ormazabal Alzola
Morocco	Aymane Jelouane   Yasmine Dridba	Sweden	Lisa Bastholm   Malin Lindgren   Michelle Smed
Norway	Godstime Ejide   Pere Alabintei	Switzerland	Paul de Blasi   Audrey Soutter   Elisabeth Zoe Everson
Panama	Jeimy Caballero   Marifé Millard	Thailand	Anthony Visate Loh   Sutthika Ruchupan   Rattanan Jaroenpornworanam
Paraguay	Daniel Fariña   Celso Santacruz   Victor Jara   Abel Coronel	The Netherlands	Rakeem Strijk
Peru	Jose Francisco Iturrizaga   Mariana Cordero   Valeria Rosell	Türkiye	Lerzan Nalbantoğlu   Hande Çağla Yılmaz   Aslı Ceyda Akdogan
Poland	Monika Skocz   Grzegorz Olszewski   Michał Mostowik   Karol Juraszczyk   Paulina Olender   Paulina Szymańska	Ukraine	Dmytro Pavlenko   Mykhailo Koliadintsev   Anastasiia Kopylchak   Anton Bychkov   Oleksii Voichyshyn   Vasyl Chopa
Portugal	João Costa da Silva   Madalena Pestana de Almeida	United Kingdom	Cavan Fabris   Katherine Eyres
Romania	Georgiana Singurel   Andreea Zaharia   Silvia Axinescu   Corina Damaschin	Uruguay	Javier Domínguez   Thaís Núñez da Rosa
Senegal	Badara Niang   Eva N’Konou	Deloitte Legal Center Of Excellence (CoE)	Ioana Niculae   Alexandra Biliuți   Julia-Maria Nedelcuț   Mihail Octavian Suciu
Serbia	Luka Trifunović   Marija Ilić		



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

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

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 457,000 people worldwide make an impact that matters at [www.deloitte.com](https://www.deloitte.com).

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

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

© 2024. For information, contact Deloitte Global.